Ingenico 6500

User's Guide

ingenico

Ingenico 6500 User's Guide
Part Number DL00458, Revision E
Released April 2006

Ingenico Inc.
1003 Mansell Road
Atlanta, GA 30076
Tel: 770.594.6000
Fax: 770.594.6003
www.ingenico-us.com

Ingenico Canada Ltd.
79 Torbarrie Road, Toronto, Ontario
Canada M3L 1G5
Tel: 416.245.6700
Fax: 416.245.6701
www.ingenico.ca

U.S. Help Desk: TotalCARE
Tel: 800.435.3014
Fax: 770.594.6026
Mon - Fri, 8:00 a.m. - 6:00 p.m.
Sat 10:00 a.m. - 3:00 p.m. EST

Canadian Help Desk: TotalCARE
Tel: 888.900.8221
Fax: 905.795.9343
Hours: Mon - Fri, 8:30 a.m. - 5:00 p.m. EST

Table of Contents

Revision History

Date	Changes	Manual Revision
2/22/06	Updated the Key Architecture chapter. Updated *Finding the Key Check Value: Terminal Keys* section by adding Special Keys option, and added new section, *Finding the Key Check Value: Application Keys*.	E
11/1/05	Updated the extended menu flow, chapters 2 through 7. Updated the IBM EFT Downloading chapter.	D
4/26/05	Changed the keys for scrolling to +, - for US.	C
2/28/05	Changed the key sequence for restarting the terminal to [1] + [CAN] + [OK]. Updated Chapter 9, Key Architecture, and Chapter 10, Secure Certificate to reflect changes to NAR SSA version 2.02, maintenance application version 1.12.	B
11/15/04	Initial Release	A

Chapter 1

Introduction

1.1 Payment Types

The Ingenico 6500 customer-activated terminal supports payment information processing and authorization at the point of sale (POS) in your business. With the appropriate application software, the Ingenico 6500 terminal supports the following payment types:

- Credit
- Debit, ATM
- Smart Card
- Electronic Benefits Transfer (EBT)

The Ingenico 6500 is also a utility platform for electronic marketing, such as advertising and loyalty programs. In addition to payment, the terminal can be used for the following:

- Customer graphics display
- Item scrolling
- Loyalty programs
- Advertising
- Instant credit
- Personal messaging
- Cross selling
- Electronic couponing

The Ingenico 6550 terminal can capture an electronic image of a customer's signature for credit transactions and transmit it to a host system (i.e., cash register or computer).

1.2 Two Terminal Models

There are two models in the Ingenico 6500 product range:

- Ingenico 6510 has four screen-addressable keys
- Ingenico 6550 has a touch screen that supports finger and stylus input and signature capture

Ingenico 6510

Ingenico 6550

The term “Ingenico 6500 terminal” will be used to refer to both the Ingenico 6510 and 6550.

1.3 Connectivity

The Ingenico 6500 terminal can connect directly to a cash register, computer, Ethernet LAN, or RS485 LAN. Peripherals such as check readers and bar code scanners can be connected to the AUX port.

For more information about connectivity, refer to the *Ingenico 6500 Installation & Operations Guide*.

1.4 About this Manual

Chapters 1 through 7 explain how to use the extended menu. Chapters 8 through 10 give background information to help you understand downloading and key management, and Chapters 11 and 12 explain how to perform a download.

Chapter 1*, Introduction*, gives an overview of the terminal, this manual, and kits that are available.

Chapter 2, *Extended Menu Overview*, explains how to navigate the extended menu and find the current setting. It also lists the options available in each menu.

Chapter 3, *System Configuration Menu*, explains how to perform the functions in the system configuration menu: change date and time, set display contrast, and adjust beep tones.

Chapter 4, *System Info Menu*, explains how to navigate through the system info menu to view the following system information: check versions, check security info, and view parameters.

Chapter 5, *Supervisor Menu*, gives the password to enter the menu, and explains how to change the password. It explains how to check or erase the application file in the terminal, and how to perform the following security functions: set key injection port, allow key injection, check the key value, and allow the serial key to be injected.

Chapter 6, *System Parameters Menu*, explains how to indicate the download method, set the download port, setup the port, and configure the host port’s auto detect feature.

Chapter 7, *Diagnostic Menu*, explains how to perform diagnostic tests on the display, keypad, beeper, communications, MSR, smart card reader, SAMs, touch screen, and signature capture.

Chapter 8, *Architecture*, explains the system architecture, host communications, and terminal architecture. It explains the components inside the terminal that are referred to in subsequent chapters.

Chapter 9, *Key Architecture*, explains the sponsor key (KTK), terminal based keys, application based keys, and security options, such as MACing.

Chapter 10, *Secure Certificate*, explains the securing process and the components of the secure certificate.

Chapter 11, *IBMEFT Download*, explains the prerequisites, preparation, timing, and steps involved with the IBMEFT method of downloading.

Chapter 12, *Download Errors*, explains how to resolve errors that might be encountered during an IBMEFT download.

1.5 Conventions Used in this Manual

The following table explains the conventions used in this manual.

Convention	Use	Example
[Brackets]	Highlights a key to press on the terminal	[1]
Bold	Highlights text that displays on the computer screen	**My Computer**
`Code`	Highlights coding used in descriptors	`MAC=12345678`
Italic	Highlights book titles, important terms, variables	*applname*

1.6 Kits

The following kits are available from your Ingenico representative, including integration and development kits used to write custom applications to run on the Ingenico 6500 terminal.

1.6.1 Basic Installation Kit

The Basic Installation Kit consists of an Ingenico 6500 terminal and an Ingenico 6500-to-ECR cable. Refer to the *Ingenico 6500 Installation and Operations Guide* for detailed instructions on installing the unit.

1.6.2 Store Installation Kit

The store installation kit consists of the contents of the Basic Installation Kit, a CD-ROM containing the Ingenico 6500 Retail Base Application program and parameter files, and a copy of the MLDT utility program.

1.6.3 Retail Base Application Integration Kit

The Retail Base Application Integration Kit consists of the Store Installation Kit, an adapter kit, and all necessary manuals. This allows for the connection of the Ingenico 6500 to an IBM PC for downloading a program or parameters using MLDT.

1.6.4 OPOS Software Development Kit

This kit contains the programs, files, and manuals needed to allow a programmer to write a custom application for a register or host that interfaces with the Ingenico 6500 using OPOS (object linking and embedding for retail point of sale).

1.6.5 JavaPOS Software Development Kit

This kit contains the programs, files, and manuals needed to allow a programmer to develop a custom application for a register or host that interfaces with the Ingenico 6500 using JavaPOS (Java for retail point of sale).

1.6.6 UNICAPT 32 Software Development Kit

This kit allows a programmer to develop a custom application for the Ingenico 6500 terminal using Ingenico's operating system, UNICAPT 32.

Chapter 2

Extended Menu Overview

2.1 Overview

The extended menu allows you to configure the terminal, get system information, check the file system, do key injection, get key check value, set system parameters for downloading, and test the product hardware. This chapter explains how to navigate the extended menu and includes a chart of menu options. Subsequent chapters explain how to perform functions in the extended menu.

2.2 Accessing the Extended Menu

To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing [1] and [3] simultaneously.

2.3 Navigating the Extended Menu

On Ingenico 6510, four lines of text can display at a time. On the Ingenico 6550, ten lines of text display. The current menu name displays on the first line, and the menu options appear on subsequent lines.

The following table lists the keys used to scroll through and select the menu options.

Note: Screen touch and screen-addressable keys cannot be used to navigate the extended menu.

Std. Key	USA Key	Action
↓	+	Scroll down one item
↑	-	Scroll up one item
Enter	Enter	Initiate selected menu option
CORR	Clear	(Correct or backspace) No effect in the extended menu
CAN/ANN	Cancel	(Cancel/annuler) Return to the previous menu If you are at the extended menu, return to application's idle prompt

Note: As you can see in the table, there are two versions of keymats: a standard version and a USA version. This manual will refer to the keys by the standard names.

The selected menu option is highlighted in reverse video. Example follows.

Display	Action
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	To select Supervisor Menu, press [↓] three times to scroll down.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Supervisor Menu is now selected. To accept, press [Enter].

2.4 Finding the Current Setting

The current setting will be highlighted in reverse video.

Display	Explanation
COM1 COM2	In this example, COM2 is the current setting.

2.5 Finding Options in the Extended Menu

Menu	Submenu	Submenu	Submenu
Serialnum Inject			
System Config	System Date/Time		
	Display Contrast		
	Key Press Beep	Enable	Length Tone
		Disable	
	Backlight On/Off	Always On	
		Always Off	
		Idle Timeout	

System Info	Versions Security Info RAM Info View Parameter			
Supervisor Menu	Change Password			
	Application File	AppA AppB	Read Erase	
	Security	Key Injection	Inject Keys	
			Injection Port	COM1 COM2
			Index Select	
			App Select	
		Key Check Value	Term Keys Application Keys	
		Erase App Keys	Key1	
			Key2	
		SerialnumInject		
	Sys Parameters	Download Method	IBMEFT NCREFT Zontalk GEMS Germany	
		Download Port	Port 1	
			Port 2	
			Port 3	
		Setup Port	Port 1	Interface Type Baud Rate Data Bits Stop Bits Parity LAN Address Retry Count Response TMO Poll TMO

				Turnaround TMO
			Port 2	Interface Type Baud Rate Data Bits Stop Bits Parity LAN Address Retry Count Response TMO Poll TMO Turnaround TMO
			Port 3	Interface Type Baud Rate Data Bits Stop Bits Parity Retry Count Response TMO DHCP Local IP Local IP Port Server IP Server IP Port IP Add Mask Gateway Primary DNS Secondary DNS Domain Name
			Dial	Dial Phone Num Modem Speed
			Host Port	COM1 COM2 COM3
			Aux Port	COM1 COM2 COM3
		Auto Detect		AD On/Off: On / Off
				AD Timeout

		Parameter Editor	AD Retry Times
Diagnostic Menu	Display		
	Keypad		
	Beeper		
	RS232	COM1	
		COM2	
	Tailgate		
	USB		
	Mag Stripe Reader		
	Smart Card Reader		
	SAM		
	Touch Screen		
	Signature Capture		
	Pen Calibration		
	Finger Calibration		
SCV Verification			

Chapter 3

System Configuration Menu

3.1 Overview

This chapter explains how to perform the functions in the system configuration menu: change date and time, set display contrast, and adjust beep tones (length and tone).

3.2 Changing the Date and Time

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [Enter] to select System Config.
System Config System Date/Time Display Contrast	Press [Enter] to select System Date/Time.
Enter Date YYYY/MM/DD 2003/08/22	Key the new date using the format YYYYMMDD, then press [Enter]. To bypass, press [Enter].
Enter Time HH:MM 17:21	Key the new time using the format, HHMM, then press [Enter]. The system uses a 24-hour clock. To bypass, press [Enter].

3.3 Changing the Display Contrast

If you are have difficulty reading your terminal screen, you can increase or decrease the contrast. This setting is stored in sysPara.cfg. You can also test the display contrast: see *Testing the Display Contrast* on page 55.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [Enter] to select System Config.
System Config System Date/Time Display Contrast	Press [↓], [Enter] to select Display Contrast.
Contrast = 100% ↑+ ↓ –	The current value is displayed, between 0 and 100. To decrease the contrast, press the [↓] key. To increase the contrast, press the [↑] key. When the desired setting is reached, press [Enter] to accept and return the configuration menu. **Note**: If you press [Can] or [CORR], the contrast setting is not changed.

Note: The terminal modifies contrast settings automatically when temperatures vary.

3.4 Changing the Beep Tones

You may disable, enable, or change the beep tones that sound when keys are pressed. These settings are stored in sysPara.cfg. To test the beep tones, see *Testing the Beeper* on page 56.

3.4.1 Enable/Disable Beep Tones

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [Enter] to select System Config.

System Config System Date/Time Display Contrast Key Press Beep	Press [↓], [↓], [Enter] to select Key Press Beep.
Beep Tone Status Enable Disable	To turn on key press beeps, press [Enter] to select Enable. To turn off key press beeps, press [↓], [Enter] to select Disable.
Key Beep Length Tone	Press [Can]. To change the beep length or tone, see the following tables. **Note**: Prompt displays if you selected Enable.

3.4.2 Changing the Beep Length

This option allows you to change how long the beep sounds on key press. To hear what each beep sounds like, see Diagnostic Menu > *Testing the Beeper*, described on page 56.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [Enter] to select System Config.
System Config Change Date/Time Display Contrast Key Press Beep	Press [↓], [↓], [Enter] to select Key Press Beep.
Beep Tone Status Enable Disable	Press [Enter] to select Enable.
Key Beep Length Tone	Press [Enter] to select Length.
Beep Length Click Short Long	Select the option you want.

Beep Length Click Short Long	Press [Can] to return to the previous menu.

3.4.3 Changing the Beep Tones

This option allows you to change the tone of the beep that sounds on key press. To hear what each beep sounds like, see Diagnostic Menu > Testing the Beeper, described on page 56.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [Enter] to select System Config.
System Config Change Date/Time Display Contrast Key Press Beep	Press [↓], [↓], [Enter] to select Key Press Beep.
Beep Tone Status Enable Disable	Press [Enter] to select Enable.
Key Beep Length Tone	Press [↓], [Enter] to select Tone.
Beep Tone Low Midtone High	Select the option you want.
Key Beep Length Tone	Press [Can] to return to the previous menu.

3.5 Turning the Backlight On or Off

3.5.1 Turning the Backlight On or Off

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [Enter] to select System Config.
System Config Change Date/Time Display Contrast Key Press Beep Backlight On/Off	Press [↓], [↓], [↓], [Enter] to select Backlight.
Backlight Always On Always Off Idle Timeout	Select Always On or Always Off.
System Configuration Updating	
Backlight Always On Always Off Idle Timeout	The current value displays in reverse video. Press [Can] to return to the previous menu.

3.5.2 Setting Backlight to Off When Idle

When the terminal is not in use, this option allows you to set an amount of time after which the backlight automatically turns off. When a customer or process engages the terminal, the backlight is turned back on.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info	Press [↓], [Enter] to select System Config.

System Config Change Date/Time Display Contrast Key Press Beep Backlight	Press [↓], [↓], [↓], [Enter] to select Backlight.
Backlight Always On Always Off Idle Timeout	Press [↓], [↓], [Enter] to select Idle Timeout.
Idle Timeout(s): Old Value: 0 Enter New Value:	Enter the new timeout value.
System Configuration Updating	
Backlight Always On Always Off Idle Timeout	Press [Can] to return to the previous menu.

Chapter 4

System Info Menu

4.1 Overview

This chapter explains how to navigate through the system info menu to view the following system information: check versions of download files, operating system, SSA, and applications; check security information such as MACing; and view parameter settings.

4.2 Finding Version Numbers

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [Enter] to select System Info.
System Info Versions Security Info	Press [Enter] to select Versions.
Versions EFTL XXXX EFTP XXXX TALIF XX.XX DIG. LDR. XX.XX.XX DIG. APP. XX.XX.XX OS XX.XX SSA XX.XX MNT APP XX.XX APP1 XX.XX	The version numbers of the download files (EFTL and EFTP), Talif chip, Digitizer loader and application, operating system (OS), System and Security Application (SSA), maintenance application (MNT APP), and all applications display. Press [↓] to scroll down to see more information. Press [Can] to return to the previous menu.

4.3 Checking the Security Information

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [Enter] to select System Info.
System Info Versions Security Info	Press [↓], [Enter] to select Security Info.
Security Info Prompt MAC Key: Terminal Based Reinject SN: Do Not Erase Keys Prompt MACing: Disable Code MACing: Disable MAC Calculation: Double Length Key Atalla KBK: Disable Startup Verify MACing: Disable PED Mode: Disable Serial Number: XXXXXXXXX	The security options and serial number display. To scroll down to read the full report, press [↓]. When you are finished reading it, press [Can] to return to the previous menu.

4.4 RAM Info

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [Enter] to select System Info.
System Info Versions Security Info RAM Info	Press [↓], [Enter] to select RAM Info.
Security Info Total RAM Size: 0 bytes Smallest Free Mem Siz: 0 bytes Biggest Free Mem Chun: 0 bytes Backup SRAM Size: 0 bytes	The security options and serial number display. To scroll down to read the full report, press [↓]. When you are finished reading it, press [Can] to return to the previous menu.

4.5 Viewing All Parameter Values

This menu option allows you to view the current system parameter settings. To change system parameters, see Chapter 6 System Parameters Menu on page 35.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [Enter] to select System Info.
System Info Versions Security Info View Parameter	Press [↓], [↓], [Enter] to select View Parameter.
View Parameters Version Info: 1.0 Key Entry Beep: Enable Key Beep Length: Click Key Beep Tone: Low Device Type: Signature Capture	The current parameter settings display. To scroll down to the next screen, press [↓]. When you are finished reading it, press [Can] to return to the previous menu. ***Note***: Your parameter values may be different.
LCD Contrast: 100% Key Inj Port: COM1 Manufacture ID: INGNAR Device Type ID: I6550N	

Backlight: Always On COM1 AutoDet Res: RS485 COM1AutoDet On/Off OFF COM1 AutoDet Timeout: 500ms	
COM1 AutoDet Retry: 3 Download Method: IBMEFT Download Port Number: COM1 Download Port Type: RS232	
Last download result: No Download COM1 Baud Rate: 9600 COM1 Data Bits: 8 COM1 Stop Bits: 1	
COM1 Parity: NONE COM1 LAN Address: 104 COM1 Retry Times: 3 COM1 Resp Timeout: 3000ms COM1 Poll Timeout: 3000ms COM1 TurnArd Timeout: 3000ms COM2 Baud Rate: 9600	

COM2 Data Bits: 8 COM2 Stop Bits: 1 COM2 Parity: NONE COM2 LAN Address: 101 COM2 Retry Times: 3	
COM2 Stop Bits: 1 COM2 Parity: NONE COM2 LAN Address: 101 COM2 Retry Times: 3	
COM2 Resp Timeout: 3000ms COM2 Poll Timeout: 3000ms COM2 TurnArd Timeout: 3000ms COM3 Baud Rate: 19200 COM3 Data Bits: 8 COM3 Stop Bits: 1 COM3 Parity: NONE COM3 Retry Times: NONE COM3 Resp Timeout: 3000ms ETH DHCP NONE/AUTO: AUTO	

ETH Local IP Add: 0.0.0.0 ETH Local IP Port: 0	
ETH Remote IP Add: 0.0.0.0 ETH Remote IP Port: 0 ETH IP Add Mask: 0.0.0.0 ETH Gateway: 0.0.0.0	
ETH Primary DNS: 0.0.0.0 ETH Secondary DNS: 0.0.0.0 ETH Domain Name: Dial Phone Num:	
Modem Speed: 9600 Appl Comment: 0.0.0.0	

Chapter 5

Supervisor Menu

5.1 Overview

This chapter explains how to change the supervisor password, check or erase the application file in the terminal, and perform the following security functions: set key injection port, allow key injection, check the key value, and allow the serial key to be injected.

5.2 Supervisor Menu Password

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter]. **Note**: If an incorrect password is entered, the message **Password Invalid** displays, then a prompt asks you to reenter the password.

5.3 Changing the Supervisor Menu Password

The password is stored in the internal SRAM.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].

Supervisor Menu Change Password Application File	Press [Enter] to select Change Password.
Enter Old Password:	Enter old password, then press [Enter].
Enter New Password:	Enter new password, then press [Enter].
New Password Again:	Enter new password again to confirm, then press [Enter].
Password Updated!	

5.4 Application File in Terminal

5.4.1 Reading the Application File

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security	Press [↓], [Enter] to select Application File.
Select Appl App A App B App C	Select the application you want to check.
Select File sysPara.cfg	Select the file.

File Menu Read Erase	Press [Enter] to select Read.
sysPara.cfg Read [SOF] 010000000000 ……	The contents of the file display. To scroll down to the next screen, press [↓]. When you are finished reading it, press [Can] to return to the previous menu.

5.4.2 Erasing the Application File

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security	Press [↓], [Enter] to select Application File.
Select Appl App A App B App C	Select the application you want to erase.
Select File sysPara.cfg	Select the file you want to erase.
File Menu Read Erase	Press [↓], [Enter] to select Erase.
Syspara.cfg Erase [SOF] 010000000000 ….	The contents of the file display. To erase, press [Enter].

Erase File? No Yes	Select YES or NO.
Erasing File	If you selected YES, the terminal confirms it is erasing the file.
Select File sysPara.cfg	If you selected NO, you are returned to the SELECT File prompt. Select another file to erase or press [Can] to return to a previous menu.

5.5 Security

5.5.1 Setting the Key Injection Port

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security	Press [↓], [↓], [Enter] to select Security.
Security Key Injection Key Check Value Erase App Keys	Press [Enter] to select Key Injection.
Key Injection Inject Keys Injection Port	Press [↓], [Enter] to select Injection Port.
Injection Port COM1 COM2 Ethernet	Select the port you want.
Updating	

5.5.2 Injecting Keys

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security	Press [↓], [↓], [Enter] to select Security.
Security Key Injection Key Check Value Erase App Keys Serialnum Inject	Press [Enter] to select Key Injection.
Key Injection Inject Keys Injection Port	Press [Enter] to select Inject Keys.
Key Injection Wait for command…	The terminal will now accept the key injection. For instructions on how to inject keys, see the manual for your key injection software (such as Ingenico's KeyFac or WinKeyFac). When finished, press [Can] to return to the previous menu.

5.5.3 Setting the Key Index

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.

Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security	Press [↓], [↓], [Enter] to select Security.
Security Key Injection Key Check Value Erase App Keys Serialnum Inject	Press [Enter] to select Key Injection.
Key Injection Inject Keys Injection Port Index Select(X)	Press [↓], [↓], [Enter] to select Index Select(X).
Index Select Old Value: X Enter New Value:	Enter the new index select value, and then press [Enter].
Key Injection Inject Keys Injection Port Index Select(Y)	The Index Select(Y) option now reflects the new index number.

5.5.4 Setting the Application Number

You will have to know the four-digit application ID number to perform this procedure.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security	Press [↓], [↓], [Enter] to select Security.

Security Key Injection Key Check Value Erase App Keys Serialnum Inject	Press [Enter] to select Key Injection.
Key Injection Inject Keys Injection Port Index Select(X) App Select(AAAA)	Press [↓], [↓], [↓], [Enter] to select App Select(AAAA).
App Select Old Value: XXXX Enter New Value:	Enter the new application select value, and then press [Enter].
Key Injection Inject Keys Injection Port Index Select(Y) App Select(BBBB)	The Index Select(BBBB) option now reflects the new application number.

5.5.5 Finding the Key Check Value: Terminal Keys

The key check value is a hexadecimal value that is used to verify that you have the right key in the terminal. You can find a key check value for terminal keys or application keys. This section covers terminal keys.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security	Press [↓], [↓], [Enter] to select Security.

Security Key Injection Key Check Value Erase App Keys Serialnum Inject	Press [↓], [Enter] to select Key Check Value.
Key Check Value Term Keys Application Keys	Select the type of key check values you want to see.
Terminal Keys Special Keys M/S Keys DUKPT Keys	Select the type of terminal key.
Special Keys Secure Text Key: 012345 Clear Text Key: 123456	The values for the keys you selected display – one of the following three screens will display.
M/S Keys Master Key 0: Session Key 0: Master Key 1: Session Key 1: etc.	
DUKPT Keys DUKPT Key 0: DUKPT Key 1: etc.	

5.5.6 Finding the Key Check Value: Application Keys

The key check value is a hexadecimal value that is used to verify that you have the right key in the terminal. You can find a key check value for terminal keys or application keys. This section covers application keys.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.

Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security	Press [↓], [↓], [Enter] to select Security.
Security Key Injection Key Check Value Erase App Keys Serialnum Inject	Press [↓], [Enter] to select Key Check Value.
Key Check Value Term Keys Application Keys	Select the type of key check values you want to see.
Application Keys APP1 APP2	Select the application you want.
APP1 Special Keys M/S Keys DUKPT Keys	Select the type of keys you want.
Special Keys Secure Text Key: 012345 Clear Text Key: 123456	The values for the keys you selected display – one of the following three screens will display.
M/S Keys Master Key 0: Session Key 0: Master Key 1: Session Key 1: etc.	
DUKPT Keys DUKPT Key 0: DUKPT Key 1: etc.	

5.5.7 Erasing Application Keys

The Erase App Keys option lists applications; you can choose to delete the keys to these applications. The applications listed no longer exist in the terminal, but the terminal has found keys that are still associated to them. These orphan keys are the only ones that the extended menu allows you to erase.

The i6500 terminal keeps the keys of deleted applications so that if a new version of the application is downloaded, the keys for that application will already be loaded in the terminal. However, if an application is no longer needed, the customer may choose to delete the keys using this menu option.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security	Press [↓], [↓], [Enter] to select Security.
Security Key Injection Key Check Value Erase App Keys Serialnum Inject	Press [↓], [↓], Enter] to select Erase App Keys.
Erase App Keys App A App B	Select the application with the keys you want to delete.
Erase App Keys? No Yes	Select Yes or No.
Processing	Displays if app keys were deleted. You are returned to the previous menu.

5.5.8 Injecting a Serial Number

Authorized repair technicians perform this procedure when replacing a damaged terminal.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security	Press [↓], [↓], [Enter] to select Security.
Security Key Injection Key Check Value Erase App Keys Serialnum Inject	Press [↓], [↓], [↓], [Enter] to select Serialnum Inject.
Inject Serial # Wait for online…	The terminal will now accept a serial number injection.

5.6 System Parameters

The system parameters are explained in the following chapter.

Chapter 6

System Parameters Menu

6.1 Overview

This chapter explains how change system parameters. These parameters allow you to indicate the download method, set the download port, setup the port, and configure the host port's auto detect feature.

To view a list of current parameter settings, see Viewing All Parameter Values on page *20*.

All system parameters are saved in the public file, sysPara.cfg, which can be read by all applications that reside in the terminal.

6.2 Setting the Download Method

Use this procedure to select IBMEFT, NCREFT, or Zontalk as your download method.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [Enter] to select Download Method.
Download Method IBMEFT NCREFT Zontalk	Select the method you want. **Note**: The default is IBMEFT.

GEMS Germany	
Updating	

6.3 Selecting the Download Port

Use this procedure to select the download port.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [Enter] to select Download Port.
Download Port Port1 Port2 Port3	Select the port that you want to use as the download port.

6.4 Setting Up the Port

6.4.1 Selecting the Download Interface Type

Use this procedure to select RS232, RS85, Ethernet, etc. as the interface type.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Download Port Port1 Port2 Port3	Select the appropriate download port (1 for Host, 2 for Aux, or 3 for E-NET).
PortX Interface Type Baud Rate Data Bits	Press [Enter] to select Interface Type.
PortX Auto Detect RS232 RS485 Tailgate USB Ethernet Dial	Select the communications method you want. If you select Auto Detect, the port will automatically detect the communications type of a cable plugged into the Host port.

6.4.2 Setting the Baud Rate

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3 Dial	Select the port you want (By default, Port 1 = Host, Port 2 = Aux, Port 3 = E-NET port - Ethernet, Dial = I.T.I.).
Port X Interface Type Baud Rate Data Bits Stop Bits	Press [↓], [Enter] to select Baud Rate. If configuring the Dial port (I.T.I. port), select Modem Speed.
Baud Rate 300 600 1200	Select the appropriate baud rate (you can scroll down to see more options).
Updating	Press [Can] to return to the previous menu.

6.4.3 Setting the Data Bits

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3	Select Port1, Port2, or Port3. (By default, Port 1 = Host, Port 2 = Aux, Port 3 = E-NET port - Ethernet.)
Port X Interface Type Baud Rate Data Bits Stop Bits	Press [↓], [Enter] to select Data Bits.
Data Bits 5 6 7 8	Select the appropriate data bits value.
Updating	

6.4.4 Setting the Stop Bits

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3	Select Port1, Port2, or Port3. (By default, Port 1 = Host, Port 2 = Aux, Port 3 = E-NET port - Ethernet.)
Set Port X Interface Type Baud Rate Data Bits Stop Bits	Press [↓], [↓], [Enter] to select Stop Bits.
Stop Bits 1 2	Select the appropriate stop bits value.
Updating	

6.4.5 Setting the Parity

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3	Select Port1, Port2, or Port3. (By default, Port 1 = Host, Port 2 = Aux, Port 3 = E-NET port - Ethernet.)
Set Port X Interface Type Baud Rate Data Bits Stop Bits Parity	Press [↓], [↓], [↓], [Enter] to select Parity.
Parity None Odd Even	Select the appropriate parity.

6.4.6 Defining the LAN Address

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2	Select Port1 or Port2. (By default, Port 1 = Host, Port 2 = Aux.)
Port X Interface Type Baud Rate Data Bits Stop Bits Parity LAN Address	Press [↓], [↓], [↓], [↓], [Enter] to select LAN Address.
LAN Address Old Value: 104 Enter New Value:	Key the appropriate LAN address, then press [Enter].

6.4.7 Setting the Retry Count

This option sets the number of times the COM port should retry in the event of failure (0 to 10).

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3	Select Port1 or Port2. (By default, Port 1 = Host, Port 2 = Aux.)
Port X Interface Type Baud Rate Data Bits Stop Bits Parity LAN Address Retry Count	Press [↓], [↓], [↓], [↓], [↓], [Enter] to select Retry Count.
Retry Count Old Value: 4 Enter New Value:	Enter the number of times the COM port should retry in the event of failure (0 to 10).

6.4.8 Setting the Response Timeout

This option sets the amount of time after which the port should cease waiting for a response, in units of 1/100 of a second.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3	Select Port1, Port2, or Port3. (By default, Port 1 = Host, Port 2 = Aux, Port 3 = E-NET port - Ethernet.)
Port X Interface Type Baud Rate Data Bits Stop Bits Parity LAN Address Retry Count Response TMO	Press [↓] six times, and then press [Enter] to select Response TMO (timeout).
Response TMO Old Value: 300 Enter New Value:	Enter an amount of time after which the port should cease waiting for a response, in units of 1/100 of a second.

6.4.9 Setting the Poll Timeout

Poll Timeout is the amount of time the host waits for a response after transmitting a device poll before it records a device poll timeout, in units of one-tenths of a second.

This time varies. It depends on the number of devices connected to the host system. The more devices connected to the host, the longer it takes the host to poll each device. If the PIN pad device misses more than 16 consecutive polls, the host will abandon the device.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2	Select Port1 or Port2. (By default, Port 1 = Host, Port 2 = Aux.)
Port X Interface Type Baud Rate Data Bits Stop Bits Parity LAN Address Retry Count Response TMO Poll TMO	Press [↓] seven times, and then press [Enter] to select Poll TMO (timeout).
Poll TMO Old Value: 300 Enter New Value:	Enter an amount of time after which the port should cease polling, in units of 1/100 of a second.

6.4.10 Setting the Turnaround Timeout

The Turnaround Timeout indicates the time a concentrator or a hub will wait between its request for data and a device's response in a poll sequence.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2	Select Port1 or Port2. (By default, Port 1 = Host, Port 2 = Aux.)
Port X Interface Type Baud Rate Data Bits Stop Bits Parity LAN Address Retry Count Response TMO Poll TMO Turnaround TMO	Press [↓] eight times, then press [Enter] to select Turnaround TMO.
Turnaround TMO Old Value: 300 Enter New Value:	Enter an amount of time after which the port should cease turnaround, in units of 1/100 of a second.

6.4.11 Defining the DHCP Address

DHCP is dynamic host configuration protocol. If the terminal is working in Ethernet mode, and if DHCP is ON, the terminal can ask the remote server to assign an IP address for it.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3	Press [↓], [↓], [Enter] to select Port3, the E-NET port - Ethernet.
Port3 Interface Type Baud Rate Data Bits Stop Bits Parity Retry Count Response TMO DHCP	Press [↓] seven times, then press [Enter] to select DHCP.
DHCP None Auto	Select None or Auto, and then press [Enter].
Updating	

6.4.12 Defining the Local IP Address

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3	Press [↓], [↓], [Enter] to select Port3, the E-NET port - Ethernet.
Port3 Interface Type Baud Rate Data Bits Stop Bits Parity DHCP Local IP	Press [↓] five times, then press [Enter] to select Local IP.
Local IP 123.456.789.012	Enter the local IP address.

6.4.13 Setting the Local IP Port Number

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3	Press [↓], [↓], [Enter] to select Port3, the E-NET port - Ethernet.
Port3 Interface Type Baud Rate Data Bits Stop Bits Parity DHCP Local IP Local IP Port	Press [↓] six times, then press [Enter] to select Local IP Port.
Local IP Port Old Value: XXXXX Enter New Value:	Enter the local IP port number.

6.4.14 Defining the Server IP Address

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3	Press [↓], [↓], [Enter] to select Port3, the E-NET port - Ethernet.
Port3 Interface Type Baud Rate Data Bits Stop Bits Parity DHCP Local IP Local IP Port Server IP	Press [↓] seven times, then press [Enter] to select Server IP.
Server IP 123.456.789.012	Enter the server IP address.

6.4.15 Setting the Server IP Port Number

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3	Press [↓], [↓], [Enter] to select Port3, the E-NET port - Ethernet.
Port3 Interface Type Baud Rate Data Bits Stop Bits Parity DHCP Local IP Local IP Port Server IP Server IP Port	Press [↓] eight times, then press [Enter] to select Server IP Port.
Server IP Port Old Value: XXXXX Enter New Value:	Enter the server IP port number.

6.4.16 Masking Your IP Address

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3	Press [↓], [↓], [Enter] to select Port3, the E-NET port - Ethernet.
Port3 Interface Type Baud Rate Data Bits Stop Bits Parity DHCP Local IP Local IP Port Server IP Server IP Port IP Add Mask	Press [↓] nine times, then press [Enter] to select IP Add Mask (IP address mask).
IP ADD MASK XXX.XXX.XXX.XXX	Enter the IP address to mask.
Updating	

6.4.17 Setting the Gateway

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3	Press [↓], [↓], [Enter] to select Port3, the E-NET port - Ethernet.
Port3 Interface Type Baud Rate Data Bits Stop Bits Parity DHCP Local IP Local IP Port Server IP Server IP Port IP Add Mask Gateway	Press [↓] ten times, then press [Enter] to select Gateway.
Gateway XXX.XXX.XXX.XXX	Enter the address of the gateway.
Updating…	

6.4.18 Setting the Primary DNS

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3	Press [↓], [↓], [Enter] to select Port3, the E-NET port - Ethernet.
Port3 Interface Type Baud Rate Data Bits Stop Bits Parity DHCP Local IP Local IP Port Server IP Server IP Port IP Add Mask Gateway Primary DNS	Press [↓] eleven times, then press [Enter] to select Primary DNS.
Primary DNS XXX.XXX.XXX.XXX	Enter the address of the Primary DNS.
Updating…	

6.4.19 Setting the Secondary DNS

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3	Press [↓], [↓], [Enter] to select Port3, the E-NET port - Ethernet.
Port3 Interface Type Baud Rate Data Bits Stop Bits Parity DHCP Local IP Local IP Port Server IP Server IP Port IP Add Mask Gateway Primary DNS Secondary DNS	Press [↓] twelve times, then press [Enter] to select Secondary DNS.
Secondary DNS XXX.XXX.XXX.XXX	Enter the address of the secondary DNS.

Updating…	

6.4.20 Setting the Domain Name

This option is reserved for future use.

6.4.21 Setting Up the Phone Number to Dial

If you are using the I.T.I port, you can define a phone number for this port to dial.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3 Dial	Press [↓], [↓], [↓], [Enter] to select Dial to configure the I.T.I. port.
Dial Dial Phone Num Modem Speed	Press [Enter] to select Dial Phone Num.
Phone Num Old Value: XXXXX Enter New Value:	Enter the server IP port number.

6.4.22 Setting Up the Modem Speed

If you are using the I.T.I port, you can define the modem speed.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3 Dial	Press [↓], [↓], [↓], [Enter] to select Dial to configure the I.T.I. port.
Dial Dial Phone Num Modem Speed	Press [↓], [Enter] to select Modem Speed.
Modem Speed 2400 4800 9600	Use the arrows to select the appropriate modem speed, and then press [Enter].
Updating	

6.4.23 Changing the Position of the Host Port or Aux Port

The ports are labeled Host, Aux, E-NET, I.T.I., and by default, Port 1 = Host, Port 2 = Aux, Port 3 = Ethernet. However, you may configure Port 1, 2, or 3 as the Host port or Aux port through this menu option. For example, if your host uses Ethernet, you may set your host port as Port 3.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port	Press [↓], [↓], [Enter] to select Setup Port.
Setup Port Port1 Port2 Port3 Dial Host Port Aux Port	Press [↓] until you reach Host or Aux port, and then press [Enter].
Dial COM1 COM2 COM3	Select the COM port you want.
Updating	

6.5 Configuring the Host Port Auto Detect Feature

By default, the Host port is set to automatically detect the communications method being used: RS232, RS485 IVI LAN protocol, RS485 Tailgate protocol, USB, or PoweredUSB.

6.5.1 Disabling or Enabling the Auto Detect Feature

By default, the Host port's Auto Detect feature is enabled.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port Auto Detect	Press [↓], [↓], [↓], [Enter] to select Auto Detect.
Auto Detect AD On/Off AD Timeout AD Retry Times	Press [Enter] to select On/Off.
AD On/Off Off On	Select the option you want.

6.5.2 Setting the Auto Detect Timeout

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port Auto Detect	Press [↓], [↓], [↓], [Enter] to select Auto Detect.
Auto Detect AD On/Off AD Timeout AD Retry Times	Press [↓], [Enter] to select AD Timeout.
AD Timeout Old Value: XXXXXXXXX Enter New Value:	Enter the amount of time after which the unit will cease trying to automatically detect the communications in the Port 1, in units of 1/100 of a second.

6.5.3 Setting the Auto Detect Retry Times

The Auto Detect Retry Times indicates how many times the terminal will attempt a communications protocol before trying the next one on the list. For example, if it is set to 3, when the terminal starts up, it will try 3 times to connect to the HOST in USB mode. If it fails, then it will try 3 times to connect to the HOST in RS485 mode. If it fails, then it will try 3 times to connect to the host in Tailgate mode. If it fails, then it will decide that COM1 is working in RS232 mode. Therefore, the less retry times, the less amount of time it will take to auto-detect the communications type.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port Auto Detect	Press [↓], [↓], [↓], [Enter] to select Auto Detect.
Auto Detect AD On/Off AD Timeout AD Retry Times	Press [↓], [↓], [Enter] to select AD Retry Times.
AD Retry Times Old Value: XXXXX Enter New Value:	The current value displays. Enter the number of times to retry the auto-detection of the Host port, from 0 to 10.

6.6 Editing Parameters

This option allows you to edit NAR SSA parameters.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu	Press [↓], [↓], [↓], [Enter] to select Supervisor Menu.
Enter Password:	Key password [2] [6] [3] [4], then press [Enter].
Supervisor Menu Change Password Application File Security Sys Parameters	Press [↓], [↓], [↓], [Enter] to select Sys Parameters.
Sys Parameters Download Method Download Port Setup Port Auto Detect Parameter Editor	Press [↓] four times, and then press [Enter] to select Parameter Editor.
Parameter ID:	Enter the parameter ID (maximum three digits).
Updating	

The following table lists the parameter ID numbers, descriptions, and values. This table is from the internal document, NAR SSA Library: Security Part, version 1.23.

The system parameter file is a public file that resides at the root directory of the terminal's System & Security Application. This file records the system parameter settings made through the supervisor menu. The financial application is allowed to read from this file.

Each parameter occupies 16 bytes in the parameter file. A null terminator is required and saved for character strings, except when the string length is 16. In such case, only 16 bytes of data are saved.

ID	Parameter Name	Description	Value	Data
0	PAR_ENABLE_KEY_BEEP	enable/disable beep tone on key entry	FALSE 0 – disable TRUE 1 – enable*	uint8
1	PAR_KEY_BEEP_LEN	beep length on key press	0xFFFFFF11 ~ 0xFFFFFF13 (HMI_BEEP_CLICK* ~ HMI_BEEP_LONG)	Uint32
2	PAR_KEY_BEEP_TONE	beep frequency on key press	0xFFFFFF01 ~ 0xFFFFFF03 (HMI_BEEP_LOW ~ HMI_BEEP_HIGH)	Uint32
3	PAR_DEVICE_TYPE	Key entry device or signature capture device.	0 – key entry device 1 – signature capture device	Uint8
4	PAR_LCD_CONTRAST	LCD contrast setting for whole device.	0~100 key entry device default contrast = 100, signature cap device default contrast =50	Uint8
5	PAR_KEY_INJ_PORT	Key injection port setting	“COM1” – com 1* “COM2” – com2 “ETH” - Ethernet	Char[5]
6	PAR_MANUFACTURE_ID	Manufacture ID	“INGNAR”*	Char[16]
7	PAR_DEVICE_TYPE_ID	Device type ID	e.g. “i6550N”, “i6510N”…	Char[16]
8	PAR_BKLT_TIMEOUT	Backlight turn off timeout	8 bytes, 0~0xFFFFFFFFFFFFFFFF*, 10ms a unit, default is always on.	Uint64
9	PAR_LCD_BACKLIGHT	LCD backlight	0-100	Uint8
10	PAR_AUTO_DET_RES	Auto detect port 1 result	AUTO_DET_RS232 0 – RS232 AUTO_DET_RS485 1 – RS485 AUTO_DET_TALIF_IVILAN 2 – TALIF IVILAN AUTO_DET_TAILGATE 3 – IBM TAILGATE AUTO_DET_USB 4 – USB	Uint8
11	PAR_AUTO_DET_ONOFF	Auto detect port 1 on or off.	FALSE 0 – off* TRUE 1 – on	Uint8
12	PAR_AUTO_DET_TIMEOUT	Auto detect port 1 timeout	4 bytes. >0, 10ms a unit.	Uint32
13	PAR_AUTO_DET_RETRY	Auto detect port 1 retry times.	1 ~ 10	Uint8
14	RESERVED	Auto detect setting reserved	N/A	

ID	Parameter Name	Description	Value	Data
15	RESERVED	Auto detect setting reserved	N/A	
16	RESERVED	Auto detect setting reserved	N/A	
17	RESERVED	Auto detect setting reserved	N/A	
18	RESERVED	Auto detect setting reserved	N/A	
19	RESERVED	Auto detect setting reserved	N/A	
20	PAR_EFTL_LEVEL_NUM	EFTL level number	0 ~ 9999	Uint16
21	PAR_EFTP_LEVEL_NUM	EFTP level number	0 ~ 9999	Uint16
22	PAR_DWL_METHOD	Download method setting	SP_DLLM_IBMEFT 0 – IBMEFT* SP_DLLM_NCREFT 1 – NCREFT SP_DLLM_ZONTALK 2 - ZONTALK SP_DLLM_GEMS 3 - GEMS SP_DLLM_GERMANY 4 – Germany Security Download	Uint8
23	PAR_DWL_PORT_NUM	Download port setting	“COM1” – COM 1* “COM2” – COM2 “COM3” – COM3	Char[5]
24	PAR_DWL_PORT_TYPE	Download port type setting	PORT_AUTO 0 – auto detect (COM1) PORT_RS232 * 1 – RS232 (COM1, COM2) PORT_RS485 2 – RS485 (COM1, COM2) PORT_TAILGATE 3 – Tailgate (COM1) PORT_USB 4 – USB (COM1) PORT_ETHERNET 5 – Ethernet (COM3) PORT_ATMODEM 6 – Dial (COM1, COM2) PORT_3201 7 – 3201 (COM1)	Uint8

ID	Parameter Name	Description	Value	Data
25	PAR_LAST_DWL_RESULT	Last download result	RES_NO_DWN_ATTEMPT * 0 - no download attempt yet. RES_DWN_OK 1- last download result successfully RES_COMM_TX_ERROR 2 - communication transmit error RES_COMM_REC_ERROR 3 - communication receive error RES_QUALIFY_BLOCK_ERROR 4 - qualify data block error RES_BAD_PROG_ERROR 5 - bad program RES_UNSUPPORT_HEADER_ERROR 6 - Unsupport eftl header file error RES_BAD_INDEX_ERROR 7 - bad program index error RES_NO_DWN_KEY_ERROR 8 - no download key error RES_SCHEDULE_DWN_ERROR 9 - fail to schedule download error RES_SEEK_BLOCK_ERROR 10 - fail seek block error RES_LOST_BLOCK_ERROR 11 - lost block error RES_GET_BLOCK_ERROR 12- fail to get block RES_DECODE_BLOCK_ERROR 13 -fail to decode block RES_CRC_ERROR 14 - crc error RES_COMPLETE_PROGRAM_ERROR 15 - fail to complete program RES_OPEN_DWN_SESSION_ERROR 16 - Fail to open download session. RES_SEND_CERTIFIC_ERROR 17 - fail to send certific data.	Uint8

ID	Parameter Name	Description	Value	Data
			RES_BDL_CFS_DWN_ERROR 18 - batch download CFS error RES_BDL_DFS_DWN_ERROR 19 – batch download DFS error RES_UPD_EFT_VER_ERROR 20 - fail to update eftl/eftp version RES_LOST_DWN_FILE_ERROR 21 - download file lost error RES_CFS_AUTH_ERROR 22 - cfs authentication error RES_CFS_DEC_ERROR 23- Cfs decryption error RES_DFS_AUTH_ERROR 24 - Dfs authentication error RES_DFS_DEC_ERROR 25 - DFS decryption error RES_FILE_WRITE_ERROR 26 - file write error RES_FILE_READ_ERROR 27 - file read error RES_NO_CFS_SPACE_ERROR 28 - cfs no space error RES_NO_DFS_SPACE_ERROR 29 - Dfs no space error RES_LOST_CERTIFIC_ERROR 30 – lost certific file error RES_UNKNOWN_ERROR 31 - unknown error RES_MEMORY_ERROR 32 – memory error RES_APP_NOT_EXIST 33 - data file application doesn't exist	
26	PAR_HOST_PORT_NUM	Port number assigned to the host interface	“COM1” – COM 1* “COM2” – COM2 “COM3” – COM3	Char[5]
27	PAR_AUX_PORT_NUM	Port number assigned to the AUX interface	“COM1” – COM1 “COM2” – COM2* “COM3” – COM3	Char[5]

ID	Parameter Name	Description	Value	Data
28	RESERVED	Download setting reserved.	N/A	
29	RESERVED	Download setting reserved.	N/A	
30	PAR_COM1_BAUD_RATE	COM1 baud rate setting	1 – COM_BAUD_50 2 - COM_BAUD_75 3 - COM_BAUD_150 4 - COM_BAUD_300 5 – COM_BAUD_600 6 – COM_BAUD_1200 7 – COM_BAUD_2400 8 – COM_BAUD_4800 9 – COM_BAUD_9600 10 – COM_BAUD_19200* 11 – COM_BAUD_38400 12 – COM_BAUD_57600 13 – COM_BAUD_76800 14 - COM_BAUD_115200	Uint8
31	PAR_COM1_DATA_BITS	COM1 data bits setting	1 - COM_DATASIZE_5 2 - COM_DATASIZE_6 3 - COM_DATASIZE_7 4 - COM_DATASIZE_8*	Uint8
32	PAR_COM1_STOP_BITS	COM1 stop bits setting	1 - COM_STOP_1* 2 - COM_STOP_2	Uint8
33	PAR_COM1_PARITY	COM1 parity setting	1 – COM_PARITY_NONE* 2 – COM_PARITY_ODD 3 – COM_PARITY_EVEN	Uint8
34	PAR_COM1_LAN_ADDRESS	COM1 LAN address setting	1 byte number, default = 0x65	uint8
35	PAR_COM1_RETRY_COUNT	COM1 failure retry count	1~10, default 3 times.	uint8
36	PAR_COM1_RESP_TIMEOUT	COM1 response timeout	4 bytes number, 10ms a unit, default = 1000	uint32
37	PAR_COM1_POLL_TIMEOUT	COM1 poll timeout	4 bytes number, 10ms a unit, default = 3000	uint32
38	PAR_COM1_TURNAROUND_TIMEOUT	COM1 turn around timeout	4 bytes number, 10ms a unit. default = 300	uint32

ID	Parameter Name	Description	Value	Data
39	PAR_COM1_INTERFACE_TYPE	COM1 connection interface type	PORT_AUTO 0 – auto detect PORT_RS232 * 1 – RS232 PORT_RS485 2 – RS485 PORT_TAILGATE 3 – Tailgate PORT_USB 4 – USB PORT_ETHERNET 5 – Ethernet PORT_ATMODEM 6 – Dial PORT_3201 7 – 3201	uint8
30 ~49	RESERVED	COM1 setting reserved.	N/A	
50	PAR_COM2_BAUD_RATE	COM2 baud rate setting	1 – COM_BAUD_50 2 - COM_BAUD_75 3 - COM_BAUD_150 4 - COM_BAUD_300 5 – COM_BAUD_600 6 – COM_BAUD_1200 7 – COM_BAUD_2400 8 – COM_BAUD_4800 9 – COM_BAUD_9600 10 – COM_BAUD_19200* 11 – COM_BAUD_38400 12 – COM_BAUD_57600 13 – COM_BAUD_76800 14 - COM_BAUD_115200	Uint8
51	PAR_COM2_DATA_BITS	COM2 data bits setting	1 - COM_DATASIZE_5 2 - COM_DATASIZE_6 3 - COM_DATASIZE_7 4 - COM_DATASIZE_8*	Uint8
52	PAR_COM2_STOP_BITS	COM2 stop bits setting	1 - COM_STOP_1* 2 - COM_STOP_2	Uint8

ID	Parameter Name	Description	Value	Data
53	PAR_COM2_PARITY	COM2 parity setting	1 – COM_PARITY_NONE* 2 – COM_PARITY_ODD 3 – COM_PARITY_EVEN	Uint8
54	PAR_COM2_LAN_ADDRESS	COM2 LAN address setting	1 byte number, default = 0x65	Uint8
55	PAR_COM2_RETRY_COUNT	COM2 failure retry count	1~10, default 3 times	Uint8
56	PAR_COM2_RESP_TIMEOUT	COM2 response timeout	4 bytes number, >0, 10ms a unit, default=1000	Uint32
57	PAR_COM2_POLL_TIMEOUT	COM2 poll timeout	4 bytes number, >0, 10ms a unit, default=3000	Uint32
58	PAR_COM2_TURNAROUND_TIMEOUT	COM2 turn around timeout	4 bytes number, >0, 10ms a unit. , default=300	Uint32
59	PAR_COM2_INTERFACE_TYPE	COM2 connection interface type	PORT_RS232 * 1 – RS232 PORT_RS485 2 – RS485 PORT_TAILGATE 3 – Tailgate PORT_USB 4 – USB PORT_ETHERNET 5 – Ethernet PORT_ATMODEM 6 – Dial PORT_3201 7 – 3201	uint8
60~69	RESERVED	COM2 setting reserved.	N/A	

ID	Parameter Name	Description	Value	Data
70	PAR_COM3_BAUD_RATE	COM3 baud rate setting	1 – COM_BAUD_50 2 - COM_BAUD_75 3 - COM_BAUD_150 4 - COM_BAUD_300 5 – COM_BAUD_600 6 – COM_BAUD_1200 7 – COM_BAUD_2400 8 – COM_BAUD_4800 9 – COM_BAUD_9600 10 – COM_BAUD_19200* 11 – COM_BAUD_38400 12 – COM_BAUD_57600 13 – COM_BAUD_76800 14 - COM_BAUD_115200	Uint8
71	PAR_COM3_DATA_BITS	COM3 data bits setting	1 - COM_DATASIZE_5 2 - COM_DATASIZE_6 3 - COM_DATASIZE_7 4 - COM_DATASIZE_8*	Uint8
72	PAR_COM3_STOP_BITS	COM3 stop bits setting	1 - COM_STOP_1* 2 - COM_STOP_2	Uint8
73	PAR_COM3_PARITY	COM3 parity setting	1 – COM_PARITY_NONE* 2 – COM_PARITY_ODD 3 – COM_PARITY_EVEN	Uint8
74	PAR_ETH_DHCP	Ethernet DHCP setting	0 – NONE* 1 – AUTO	Uint8
75	PAR_ETH_LOCAL_IP_ADD	Ethernet local IP address setting	4 bytes contain the IP address	Uint8 [4]
76	PAR_ETH_LOCAL_IP_PORT	Ethernet local IP port	2 bytes number.	Uint16
77	PAR_ETH_REMOTE_IP_ADD	Ethernet remote IP address setting	4 bytes contain the IP address	Uint8 [4]
78	PAR_ETH_REMOTE_IP_PORT	Ethernet remote IP port	2 bytes number	Uint16
79	PAR_COM3_RETRY_COUNT	COM3 failure retry count	1~10, default 3 times	Uint8
80	PAR_COM3_RESP_TIMEOUT	COM3 response timeout	4 bytes number, >0, 10ms a unit, default=1000	Uint32
81	PAR_ETH_MASK	Ethernet mask	4 bytes	Uint8 [4]

ID	Parameter Name	Description	Value	Data
82	PAR_ETH_GATEWAY	Ethernet gateway	4 bytes	Uint8 [4]
83	PAR_ETH_PRIM_DNS	Ethernet primary dns	4 bytes	Uint8 [4]
84	PAR_ETH_SECN_DNS	Ethernet secondary dns	4 bytes	Uint8 [4]
85	PAR_ETH_DOMAIN	Ethernet domain name	maximum length of 16 bytes	char[17]
86	PAR_COM3_INTERFACE_TYPE	COM3 connection interface type	PORT_RS232 1 – RS232 PORT_RS485 2 – RS485 PORT_TAILGATE 3 – Tailgate PORT_USB 4 – USB PORT_ETHERNET * 5 – Ethernet PORT_ATMODEM 6 – Dial PORT_3201 7 – 3201	uint8
87 ~89	RESERVED	COM3 setting reserved.	N/A	
90 ~99	RESERVED	Reserved parameters	N/A	
100	PAR_MODEM_PHONE_NUM	Modem phone number	maximum length of 16 bytes	char[17]
101	PAR_MODEM_SPEED	Modem speed	1 – COM_BAUD_50 2 - COM_BAUD_75 3 - COM_BAUD_150 4 - COM_BAUD_300 5 – COM_BAUD_600 6 – COM_BAUD_1200 7 – COM_BAUD_2400 8 – COM_BAUD_4800 9 – COM_BAUD_9600 10 – COM_BAUD_19200	uint8

ID	Parameter Name	Description	Value	Data
			11 – COM_BAUD_38400 12 – COM_BAUD_57600 13 – COM_BAUD_76800 14 - COM_BAUD_115200	
102~ 109	RESERVED	Reserved for modem settings	N/A	
110	PAR_APPL_COMMENT	Application comment	maximum length of 16 bytes	char[17]
111~ 126	RESERVED	Reserved parameters	N/A	
127	PAR_VER_REV_INFO	Version/Revision information for system parameter file.	Maximum length of 16 ASCII bytes, the format is 1byte 1byte 14byte ‘ V R Comments’	Char[17]

Chapter 7

Diagnostic Menu

7.1 Overview

This chapter describes the diagnostic tests that the customer can perform on the Ingenico 6500. The diagnostic tests allow you to isolate failures in field-installed Ingenico 6500 units. These tests are part of the operating system and are not changed by applications. The diagnostics are menu-driven with features that allow a logical progression through the tests. Once a test is selected, a test or a series of tests will be performed on the selected entity. The result of the test will be displayed to facilitate diagnosis of the malfunctioning parts.

7.2 Testing the Display Contrast

To change the display contrast, see *Changing the Display Contrast* on page 12. To test the display contrast, follow this procedure. This test tests all pixels to see if they are working.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu Diagnostic Menu	Press [↓], [Enter] to select Diagnostic Menu.
Diagnostic Menu Display Keypad	Press [↓], [Enter] to select Display.
	The pixels are tested to determine if any are not working, or are stuck on. The unit goes through the following sequence: All pixels on – White screen displays. Every other pixel off – Light gray screen displays. All pixels off – Dark gray screen displays. Every other pixel on – Light gray screen displays.

7.3 Testing the Keypad

This allows you to test each key to ensure the proper value returns.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu Diagnostic Menu	Press [↓], [Enter] to select Diagnostic Menu.
Diagnostic Menu Display Keypad	Press [↓], [Enter] to select Keypad.
Keypad 0 (0x30) To exit, press “CAN”	Press a key to test. (Here, we pressed 0). The key value and hexadecimal value stored in the terminal’s memory returns. When finished, press [CAN].

7.4 Testing the Beeper

This feature tests the beeper by sounding and displaying each possible beep type.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu Diagnostic Menu	Press [↓], [Enter] to select Diagnostic Menu.
Diagnostic Menu Display Keypad Beeper	Press [↓], [Enter] to select Beeper.

Beeper Length of beep: Click/Short/Long Frequency of beep: Low/Midtone/High	The terminal displays and sounds each possible beep type.

7.5 Testing the RS232 Connection

This feature tests the RS232 connection.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu Diagnostic Menu	Press [↓], [Enter] to select Diagnostic Menu.
Diagnostic Menu Display Keypad Beeper RS232	Press [↓], [Enter] to select RS232.
RS232 COM1 COM2	Select the communications port to test.
RS232 Host 19200, None, 8 Test	The results of the test display. Press [Can] to exit.

7.6 Testing the RS485 Tailgate Connection

This feature tests the RS485 Tailgate connection on the HOST port.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu Diagnostic Menu	Press [↓], [Enter] to select Diagnostic Menu.
Diagnostic Menu Display Keypad Beeper RS232 Tailgate	Press [↓], [Enter] to select Tailgate.
Tailgate IBM 46xx Test 2A23 (0x68)	The results of the test display. To exit, press [Can].

7.7 Testing the USB Port

This feature tests the USB connection.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu Diagnostic Menu	Press [↓], [Enter] to select Diagnostic Menu.
Diagnostic Menu Display Keypad Beeper RS232 Tailgate USB	Press [↓], [Enter] to select USB.
USB Diagnostic Connect USB Port OK Start PC App then Push OK Key to send	1. From the HOST, start uloop.exe. 2. From the terminal, press [Enter].
USB Diagnostic MESSAGE n Send . . .	The results of the test display. To exit, press [Can].

7.8 Testing the Magnetic Stripe Reader

This feature tests the magnetic stripe reader.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu Diagnostic Menu	Press [↓], [Enter] to select Diagnostic Menu.
Diagnostic Menu Display Keypad Beeper RS232 Tailgate USB Mag Stripe Reader	Press [↓], [Enter] to select Mag Stripe Reader.
Mag Stripe Reader Swipe Card Now	Swipe a magnetic stripe card.
Mag Stripe Reader 3 tracks read, track 1 Info: isoTrackNumber=4, isoStatus=ffffebff isoLength=0	The terminal displays the results of the test for each track.

7.9 Testing the Smart Card Reader

This feature tests the smart card reader.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu Diagnostic Menu	Press [↓], [Enter] to select Diagnostic Menu.
Diagnostic Menu Display Keypad Beeper RS232 Tailgate USB Mag Stripe Reader Smart Card Reader	Press [↓], [Enter] to select Smart Card Reader.
Smart Card Reader Insert Card Now	Insert a smart card.
Smart Card Reader SynchXXX card	The terminal displays the results of the smart card test.
Smart Card Reader Please remove the card!	Remove the card.

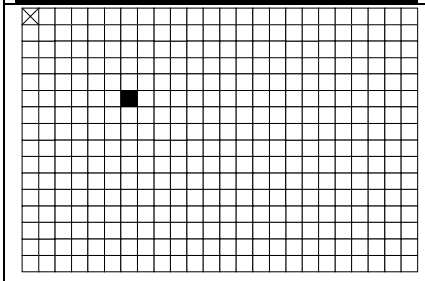
7.10 Testing the SAMs

This feature tests communication between the SAM slots and the SAM micro-controller (SMC).

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu Diagnostic Menu	Press [↓], [Enter] to select Diagnostic Menu.
Diagnostic Menu Display Keypad Beeper RS232 Tailgate USB Mag Stripe Reader Smart Card Reader SAM	Press [↓], [Enter] to select SAM.
SAM Found SAM Slot1. Found SAM Slot2. Found SAM Slot3. Found SAM Slot4.	
SAM Check Slot2 ATR Read data from Slot2 (Result)	ATR means answer to reset.
SAM Power off all slots Close all smc slots	SMC stands for SAM micro-controller.

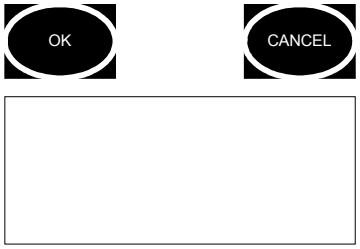
7.11 Testing the Touch Screen

This feature displays a grid. When you touch anywhere on the screen, a box on the grid is darkened. This test is for the i6550 only.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu Diagnostic Menu	Press [↓], [Enter] to select Diagnostic Menu.
Diagnostic Menu Display Keypad Beeper RS232 Tailgate USB Mag Stripe Reader Smart Card Reader SAM Touch Screen	Press [↓], [Enter] to select Touch Screen.
	This feature displays a grid. When you tap the screen, a box on the grid is darkened to let you know where you tapped. This allows you to test a portion of the screen you suspect may be having problems. ***Note***: To return to the previous menu, tap the X in the top left corner.

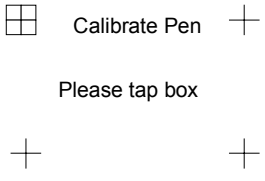
7.12 Testing Signature Capture

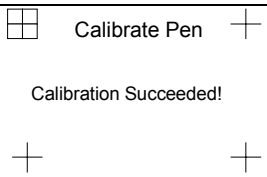
This feature displays a signature capture screen, so you can test how a signature inks and displays on the screen. This test is for the i6550 only.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu Diagnostic Menu	Press [↓], [Enter] to select Diagnostic Menu.
Diagnostic Menu Display Keypad Beeper RS232 Tailgate USB Mag Stripe Reader Smart Card Reader SAM Touch Screen Signature Capture	Press [↓], [Enter] to select Signature Capture.
	This feature displays a signature capture screen, so you can test how a signature inks and displays on the screen. When finished, tap **OK**.

7.13 Testing Pen Calibration

If your terminal is not correctly interpreting pen touches, use this test to adjust the pen calibration. This test is for the i6550 only.

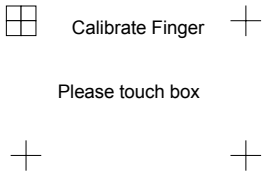
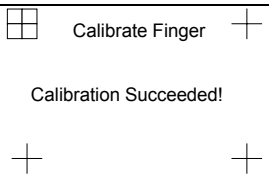
Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu Diagnostic Menu	Press [↓], [Enter] to select Diagnostic Menu.
Diagnostic Menu Display Keypad Beeper RS232 Tailgate USB Mag Stripe Reader Smart Card Reader SAM Touch Screen Signature Capture Pen Calibration	Press [↓], [Enter] to select Pen Calibration.
Please remove hands/objects from around the display **Calibration will start in 3 seconds…**	
	Using the stylus, tap the four-box grid. The box moves around to the next corner; tap again. Repeat until you are notified if the test was successful.

	You are notified if the calibration succeeded or failed.

7.14 Testing Finger Calibration

If your terminal is not correctly interpreting finger touches, use this test to adjust the finger calibration. This test is for the i6550 only.

Display	Action
	To access the extended menu, restart the terminal by pressing [1] + [CAN] + [OK]; while the terminal is starting up, access the extended menu by pressing the [1] and [3] keys simultaneously.
Extended Menu Serialnum Inject System Config System Info Supervisor Menu Diagnostic Menu	Press [↓], [Enter] to select Diagnostic Menu.
Diagnostic Menu Display Keypad Beeper RS232 Tailgate USB Mag Stripe Reader Smart Card Reader SAM Touch Screen Signature Capture Pen Calibration Finger Calibration	Press [↓], [Enter] to select Finger Calibration.
Please remove hands/objects from around the display, calibration will start in 3 seconds…	

	Using your finger, touch the four-box grid. The box moves around to the next corner; touch again. ***Tip***: For the calibration to succeed, you need to touch the buttons from the side: Touch the left buttons with your left hand and the right buttons with your right hand. Repeat until you are notified that the test was successful.
	You are notified if the finger calibration was successful. If calibration failed, try again, making sure to follow the preceding tip.

7.15 SCV Verification

This test is for internal Ingenico use only.

Chapter 8

Architecture

8.1 Overview

To understand downloading, it helps to understand the architecture of the Ingenico 6500 terminal. Terms explained in this chapter are used in the subsequent chapters. This chapter explains the system architecture, how the unit connects to the host device, and the terminal's architecture.

8.2 System Architecture

The server (local or remote) sends information to the store controller (if present), which sends it to each host or point of sale device - typically an electronic cash register (ECR), and each ECR sends it to the Ingenico 6500 terminal attached to it. The Ingenico 6500 terminal in turn sends information back through the chain. Figure 1 and Figure 2 illustrate the information flow for stores with and without a store controller.

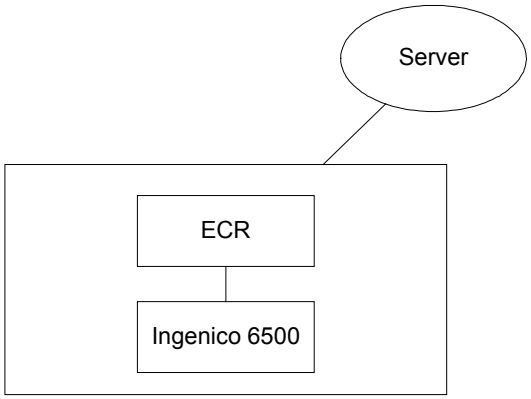


Figure 1 Single Unit Architecture

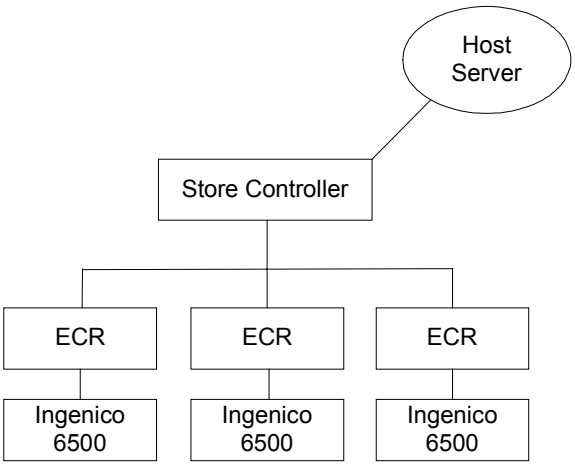


Figure 2 Multiple Unit Architecture

8.3 Host Connections

The point of sale (POS) system, which can be comprised of the server, store controller, and host devices, communicates with the Ingenico 6500 terminal through an RS-232 or RS-485 serial interface, Ethernet LAN, or USB, depending on the requirements of the host device (typically a computer or ECR). Data is sent using one of these interfaces over a cable that connects the host device to the Ingenico 6500 terminal.

The Ingenico 6500 terminal can connect directly to a cash register, computer, Ethernet LAN, or RS485 LAN. Peripherals such as check readers and printers can be connected to the AUX port.

Depending on your configuration, there are two to four communication ports.

The HOST port, which connects to POS terminals, can connect to the following protocols: RS232, USB/PoweredUSB, RS485 IVI LAN protocol, or RS485 Tailgate protocol (North America only).

The AUX port is RS232 for connecting an auxiliary device such as a printer or check reader.

The E-NET port (Ethernet 10 base T, TCP/IP) is available on certain configurations.

The ITI port is for ISDN and is available in Germany.

Note: For instructions on making these connections, refer to the *Ingenico 6500 Installation Guide*.

8.4 Terminal Architecture

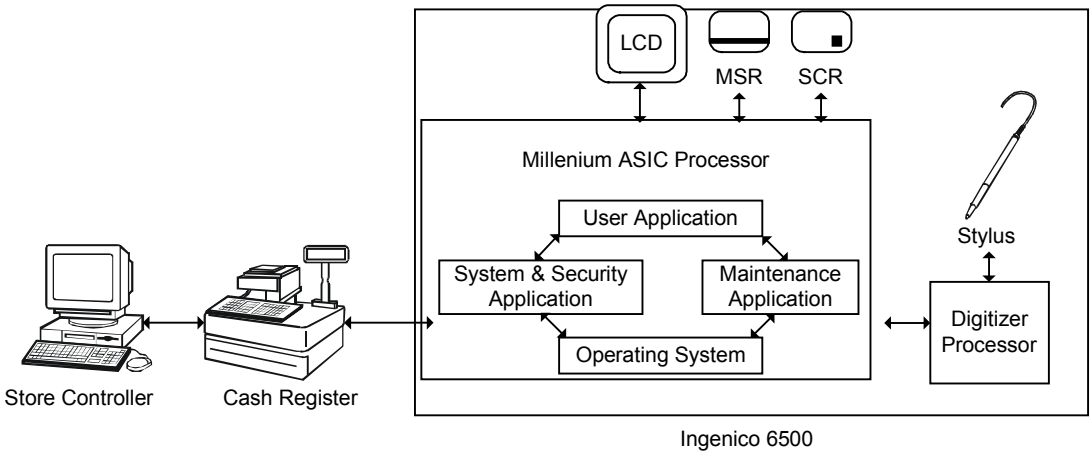


Figure 3 Terminal Architecture

As illustrated in Figure 3 Terminal Architecture, the Millennium ASIC processor runs programs that act as an interface between the ECR and the Ingenico 6500 terminal: the operating system, system and security application, maintenance application, and user application.

8.4.1 Operating System

The operating system is comprised of several elements. Some of the more prominent ones are explained in this section.

Code File System
The operating system is separated in several code files, and any application can be implemented as one or several code files. Code files can be run and downloaded independently from each other. The Code File System (CFS) manages the storage of all code files in flash devices. A configuration file lists all the code files composing and describing an application. The System & Security Application manages the CFS.

Data File System
The Data File System (DFS) manages storage and organization of permanent data. The DFS enables each application to create directories and to store data in files inside flash devices.

Human Machine Interface
The Human Machine Interface (HMI) peripheral allows applications to interface to the human element of the system through the sensory input/output devices present in the system, such as the display, keypad, and buzzer.

Memory Management Unit
The Memory Management Unit (MMU) controls memory access permissions, aborting illegal accesses. It protects the memory of the operating system and of each application, so that applications cannot access or destroy data and code in the operating system or in other applications.

Each application is fire walled from the other applications using the MMU. Each application runs in its own MMU virtual context that prevents any other applications from accessing its data. The operating system runs inside its own MMU virtual context in supervisor mode. Each application runs inside its own MMU virtual context in user mode. The MMU translates these virtual addresses into physical addresses. The MMU presents the physical memory locations to a program so it can access the code and data. This partitioning prevents any application from accessing other application data or operating system data.

All applications are linked at the same virtual address using the MMU. This allows independent development of all applications using the same framework. However, communications between applications are not completely prevented; they are managed through the PAM.

Application Manager Peripheral
The Application Manager peripheral (PAM) is the main component of the multi-application management system. It is in charge of the management of all UNICAPT32 native applications, which run in the operating system simultaneously. The PAM provides mechanisms that allow synchronization between applications and exchange of data.

System and Security Application
The System and Security Application (SSA) has two modules.

- The system module contains the terminal's extended menu, where users can change options related to downloading, diagnostics, system parameters, and system configuration.
- The security module implements all security requirements, such as key injection and key management. The cryptography functions of the operating system, including key storage areas, are only accessible to the security module. The security module provides a cryptography API to other applications. The SSA blocks any user applications from using the HMI peripheral of the operating system. Thus, all requests by the user application to display forms or receive touch or stylus input must go through the SSA. The SSA then rejects any improper insecure requests, such as:
    - Activate more than 8 screen buttons (which could be used to create a false PIN pad).
    - Activate PIN entry with a prompt that has no valid MAC (if the MACing option is on; this prevents the improper collection of the encryption results of known data).
    - Activate clear text entry with a prompt that has no valid MAC (if the MACing option is on).
    - Activate clear text entry with a prompt that contains words such as PIN, NIP, etc. (if the MACing option is off).
    - Retrieve pixel coordinates of individual screen touches (which could be used to create a false PIN pad).
    - Request more than 30 PIN encryptions within 15 seconds when using MASTER PIN KEY.

Maintenance Application
The maintenance application is in charge of system components and secure application download. It is an extension of the SSA and the SSA invokes it. It executes before other user applications in order to check version numbers and download new software if needed.

The maintenance application communicates with the user application through the peripheral application manager (PAM). The maintenance application has a downloader that communicates with the host in the specified download protocol to receive data and send responses. Each download protocol has its own download application.

The maintenance application sends the code files and application data files it receives to the data file system (DFS) first. At the end of download, it releases the COM port, and then requests an offline download from the SSA. The SSA maintenance module performs a security call back to decrypt, unzip, and authenticate the code before it writes the code file to the code file system (CFS). Also, it takes the data files from DFS, goes through the call back function to authenticate it, and puts them in the right place within the DFS.

The download port selection, download protocol, and port setting can be set in the supervisor menu (see Chapter 5, *Supervisor Menu,* on page 23).

User Application
A user application controls the terminal through customer-specific forms and prompts. User applications are also called payment applications or financial applications. There can be a single user application or multiple ones. User applications vary widely. An application may be thick and contain much business logic, or it may be a thin layer that simply passes on requests from the register. Ingenico provides standard user applications intended for certain markets, or you can create your own user applications using Ingenico's Ingedev application development environment. In the North American market, standard user applications include Retail Base Application and UPOS interface application.

A user application accesses secure functions, such as the display screen, screen buttons, terminal keys, and signature capture, through the security module of the SSA. For all other functions, such as port communications, smart card, and magnetic stripe reader, the user application accesses the operating system directly.

8.4.2 Digitizer

The digitizer is a chip with software on it that handles the interface with the user. It receives finger and stylus input from the display screen, which it sends to the operating system, where it goes first to the human machine interface to be processed. The HMI sends the data to the SSA for security screening. The SSA sends it to the user application.

8.4.3 Transmitting Data

The operating system receives commands from the host (through a port), magnetic stripe reader (MSR), and smart card reader and sends them to the user application. Secure functions, such as display screen, screen buttons, terminal keys, and signature capture, are sent to the SSA for security screening before being sent to the user application.

The user application controls the terminal through customer-specific forms and prompts that it sends to the SSA for security screening. The SSA then sends the data to the display screen. The user application uses the operating system to send and receive messages to the host through a port.

The operating system provides the user application with debit and credit card information from the MSR and stored value from the smart card reader. The operating system encrypts the user PIN. This encrypted information is sent from the operating system to the user application. From the user application, it goes from the cash register to the store controller, and then on to banks and other processors.

The digitizer handles the interface with the user. It receives input from the touch screen and translates it into data that the operating system and SSA can process and encrypt.

8.5 Download File Architecture

The download file is installed on the server. The customer is responsible for sending the code from the server to the electronic cash registers (ECRs). Each ECR sends the code to its Ingenico 6500 terminal.

On the POS system, two software components are required:

- Files to be downloaded to the Ingenico 6500 terminal
- Downloader, specific to the cash register. Ingenico supports several formats including:
    - IBM EFT download format
    - NCR download format
    - GEMS and GEMS Lite

Chapter 9

Key Architecture

9.1 Overview

This chapter is extracted from the document NAR System & Security Application (SSA) Software Architecture, Key Architecture section, revision 1.19.

Figure 4 on page 75 provides an overview of the Ingenico 6500's key architecture. A default key is used for the highest level, Sponsor Key KTK (Key Transfer Key). Customers can change the sponsor key. Figure 4 shows the sponsor key under the terminal ID because the sponsor key is unique per terminal.

All keys indicated are loaded by the financial institution or authorized injection facility. The cryptographic keys must be injected into the i6500 terminal in a Key Secure Room. The KTK is the only key that can be transported in the clear between the Key Injection Utility and the device. The rest of the keys may be generated randomly, entered in the system as cryptograms, or entered by key parts using principles of both split knowledge and dual control.

Use a key injection utility, such as Ingenico's WinKeyFac software program, to perform these functions and to set security options (see Security Options on page 77).

Financial keys (Master/Session and DUKPT) can be based on an application or a terminal. By default, all financial keys are based on an application, as shown in Figure 4. By changing the value of the Financial Key security option (see section 9.5.9 Financial Key Option on page 99), you can make all financial keys based on a terminal; however, this will erase all previously injected financial keys.

Some keys are segregated by application. The application number is part of the application name. Once the keys are injected, the application number is used as the application reference. When the application calls a cryptographic function, it passes the application reference as the application name. The SSA will check that the caller passes the application name, and from the name, it will determine the number that defines the injected key set.

Single-length DES keys have a length of 8 bytes. Double-length triple DES keys have a length of 16 bytes. The *level* of the specific key set indicates the position of the key set in the internal key hierarchy. For example, keys at Level 1 (sponsor keys) are loaded in clear text and sit at the top of the key hierarchy. Keys at Level 2 are loaded encrypted under the keys at Level 1. Keys at Level 3 are loaded encrypted under the keys at Level 2. Loading a key at a higher level will cause the erasure of all the related lower level keys. The following sections describe each key.

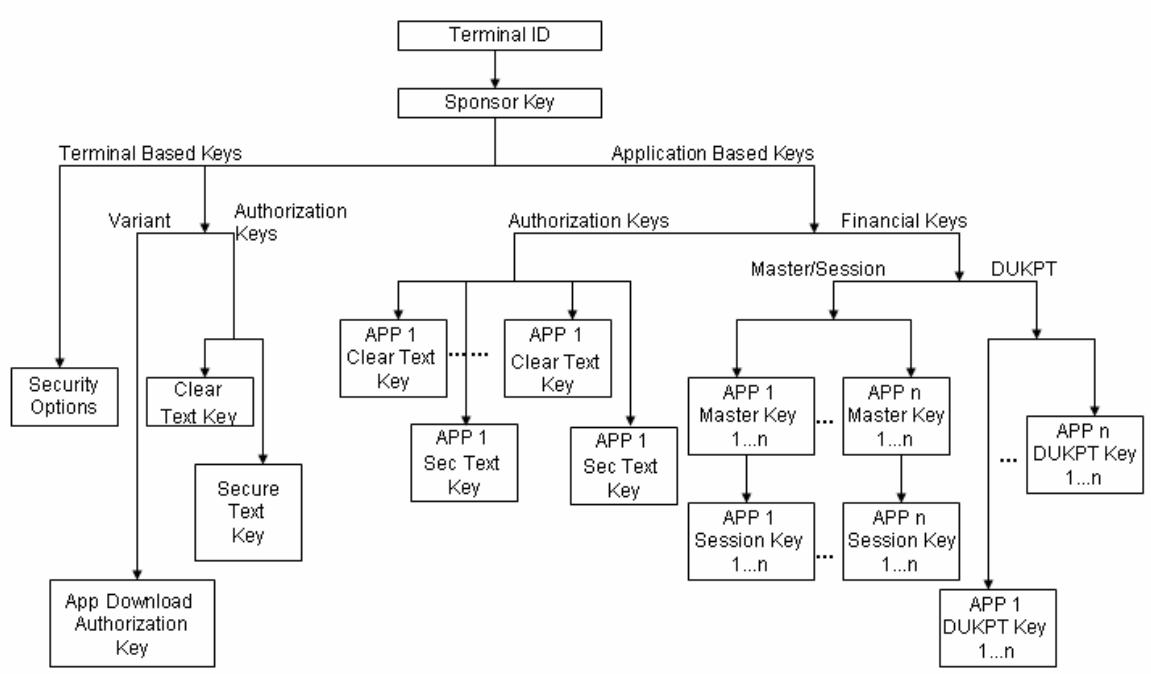


Figure 4 Key Architecture

9.2 Sponsor Key (KTK)

Key Name	Index	Length	Description of Key
Sponsor key (KTK, key transfer key, also known as TMK)	0	16	This key will be loaded as clear text. All Level 2 keys will be transferred to the debit terminal encrypted under this key. A default key is set if no customer key is injected.

9.3 Terminal Based Keys

Key Name	Index	Length	Description of Key
Secure Text Entry Form Authorization Key (PEFMK)	1	8/16	This key is loaded encrypted under the KTK. All prompts and/or screens used for Secure Text Entry of all applications will be authenticated using this key if the Prompts Authentication Key security option is set to terminal based (0).
Clear Text Entry Form Authorization Key (CEFMK)	2	8/16	This key is loaded encrypted under the KTK. All prompts and/or screens used for Clear Text Entry of all applications will be authenticated using this key if Prompts Authentication Key security option is set to terminal based (0).
Application Download Authorization Key (CDMK)	3	8/16	This key is the variant of KTK. It will be used to verify the MAC value of the fingerprint of the code being downloaded into the device. Code MACing always uses the Application Download Authorization Key.

9.4 Application Based Keys

9.4.1 Special Keys

Special keys are loaded encrypted under the KTK. The SSA will have a key structure matrix indexed by application ID. These keys can be both single-length DES keys and double-length triple DES keys.

These two Application Special Keys are only used if the Prompts Authentication Key security option is set to 1 (application based, see section 9.5.1 on page 96). If Prompt MACing is also enabled, the Secure Text and Clear Text prompts will be verified with these two keys. If the Prompts Authentication Key is set to 0 (terminal based), the terminal-based keys are used instead (see section 9.3 on page 93).

Key Name	Index	Length	Description of Key
Secure Text Entry Form Authorization Key	1	8/16	This key is loaded encrypted under the KTK. All prompts and/or screens used for Secure Text Entry of the application will be authenticated using this key if the Prompts Authentication Key security option is set to application based (1).
Clear Text Entry Form Authorization Key	2	8/16	This key is loaded encrypted under the KTK. All prompts and/or screens used for Clear Text Entry of the application will be authenticated using this key if the Prompts Authentication Key security option is set to application based (1).

9.4.2 Master Keys

Master keys are loaded encrypted under the KTK or current Master Key. For application-based financial keys, the SSA will have a key structure matrix indexed by application ID.

The device can accommodate up to ten master keys per application, or 64 master keys per terminal. Each key is independent and used to transport the corresponding working (session) key. Available indexes for master keys are 0 – 9 per application or 0 – 63 per terminal. These keys can be both single-length DES keys and double-length triple DES keys.

The device supports four types of master keys.

Key Name	Description of Key
Master Terminal PIN Key (MTPK)	This key is used to encrypt the Working (session) Terminal PIN Key (WTPK).
Master Message Authentication Code Key (MMACK)	This key is used to encrypt the Working (session) Message Authentication Code Key (WMACK).
Master Communication Key (MCK)	This key is used to encrypt the Working (session) Communication Key (WCK).

Key (MCK)	
Master Atalla Key	This key is used to XOR a value for PIN entry, MAC, or encrypt/decrypt to form master variant keys to decrypt for PIN entry, MAC, and COM session keys.

9.4.3 Session Keys

These keys are loaded encrypted under the corresponding master keys. This means that the type and index of the working (session) key have to match the type and index of the corresponding master key that was used to encrypt it. For application based financial keys, the SSA will have a key structure matrix indexed by application ID.

The device can accommodate up to ten working (session) keys per application, or up to 64 working (session) keys per terminal. Available indexes for the working (session) keys are 0 – 9 per application or 0 – 64 per terminal. These keys can be both single-length DES keys and double-length triple DES keys. Similar to the master keys, the device supports four types of working (session) keys.

Key Name	Description of Key
Working (session) Terminal PIN Key (WTPK)	This key is loaded encrypted under the corresponding Master Terminal PIN Key. It is used to encrypt the customer PIN for transmission to the host.
Working (session) Message Authentication Code Key (WMACK)	This key is loaded encrypted under the corresponding Master Message Authentication Code Key. It is used to authenticate the customer transaction.
Working (session) Communication Key (WCK)	This key is loaded encrypted under the corresponding Master Communication Key. It is used to encrypt customer transaction data between the debit terminal and the host.
Working (session) Atalla Key	This key is decrypted by the Master Atalla Variant Key, which is created from the Master Atalla Key according to the type of operation to be performed.

9.4.4 DUKPT Keys

The Initial PIN Pad Keys (IPPKs) are loaded encrypted under the KTK. The device can accommodate up to ten separate DUKPT engines. Each engine is initialized with an IPPK. Available indexes for the DUKPT engines are 0 – 9. The IPPKs can be both single-length DES keys and double-length triple DES keys.

9.5 Security Options

This section provides a synopsis of each security option. All the security options can be loaded during key injection. The user application can request the security options setting from an SSA API.

9.5.1 Prompts Authentication Key Options

This option controls whether the prompt authentication keys are based on the terminal or the application. These options will be used when doing any secure data entry.

When prompt MACing is enabled and the prompts authentication key security option is set to 0 (terminal based), at data entry time, the secure text and clear text prompts will be verified with the terminal-based special keys.

When prompt MACing is enabled and the prompts authentication key security option is set to 1 (application based), at data entry time, the secure text and clear text prompts will be verified with application based special keys.

Possible Values	Description
0	Prompts authentication key is terminal based. If Prompt MACing is also enabled, the form's prompt display will be authenticated by the terminal-based clear text key and security text key. (Default)
1	Prompts authentication key is application based. The form's prompt display is authenticated by an application-based clear text key or a security text key.

9.5.2 Change Terminal ID Option

This option controls the financial keys existence once the terminal ID is re-loaded.

Possible Values	Description
0	Changing Terminal ID will not erase all keys. (Default) Once the terminal ID is re-injected through the key injection process, the existing keys will be retained.
1	Changing Terminal ID will erase the keys. Once the terminal ID is re-injected, all of the financial keys, including Master/Session and DUKPT keys, will be erased.

9.5.3 Prompt MACing

Prompt MACing controls how a data entry form's display prompts are shown.

Possible Values	Status	Description
0	Disabled	Prompts are not authenticated before being displayed the screen. (Default)
1	Enabled	Prompts are authenticated and then displayed on the screen.

Prompt MACing uses a key that depends on how the form/prompt authentication option is set. If set to:

- Terminal based, Prompt MACing will use terminal based clear text key if the form is set to clear text entry. It will use the terminal-based security text key if the form is set to secure text entry.
- Application based, Prompt MACing will use application based clear text key if the form is set to clear text entry. It will use the application-based security text key if the form is set to security text entry.

Prompt MACing will be used to authenticate the prompts during the data entry process and the load font process.

9.5.4 Code MACing

Code MACing controls how code files are updated.

Possible Values	Status	Description
0	Disabled	No authentication is performed on code file updates. (Default)
1	Enabled	Special authentication is performed on code file updates.

Code MACing verifies that only certified applications and files are loaded into the device.

During security download, if Code MACing is enabled, all the code files will be authenticated after they are downloaded. The authentication method is given in the certificate file, which includes NONE, SHA1+MAC, MAC, etc.

9.5.5 Double-Length Key MAC Calculation

This option controls how the MAC calculation algorithm operates when the MAC key is a double-length key. This setting only applies to MAC calculation in financial transactions.

Possible Values	Encryption	Description
0	EDE (encrypt, decrypt, encrypt)	Double-length key encryption on each block of data. (Default)
1	E (encrypt)	Single-length key encryption on each block of data, except for the last block, which uses EDE encryption.

9.5.6 Atalla Key Block Protection Option

This option controls whether the double-length master/session key injection is protected by the Atalla key block injection. If the option is enabled, double-length master or session key can only be injected through Atalla key block.

Possible Values	Status	Description
0	Disabled	No protection is applied. Double-length master/session key can be injected through any format. (Default)
1	Enabled	Protection is applied. ▪ Double-length master key and double-length session key can only be injected through Atalla key block. They cannot be injected through the normal key format. ▪ Single-length master/session keys, Atalla key block format keys, single or double feature keys, and single or double DUKPT keys can be injected through both the normal key format and Atalla key block format.

9.5.7 Terminal Startup Verify MAC Option

This option controls whether the terminal needs to verify the MAC at terminal startup for user application code files and data files that are contained in a valid certificate file. The default value is disabled because the manufacturer does not load the certificate file.

Possible Values	Status	Description
0	Disabled	Disable startup verify MAC option. (Default)
1	Enabled	Enable startup verify MAC option.

9.5.8 Visa PED Mode Option

This option controls whether the terminal runs in Visa PED mode. In this mode, if prompt MAC verification fails, PIN exhaustion validation and the three button limit will be applied when prompt MAC verification fails.

- PIN exhaustion validation means that the customer can only enter their PIN three times; after the third failed attempt, the terminal returns to the idle prompt.
- The three button limit means that forms that do not have Prompt MACing are limited to three buttons. If the form requires more than three data inputs, such as PIN entry or cash back amount, it must have prompt MACing.

Possible Values	Status	Description
0	Disabled	Normal mode.
1	Enabled	Visa PED mode.

9.5.9 Financial Key Option

This option controls whether the financial keys are application based or terminal based.

Caution: If you change this security option, previously loaded financial keys will be lost.

Possible Values	Status	Description
0	Disabled	Financial keys are application based. (Default) For application based financial keys, SSA supports 10 Master/Session keys and 10 DUKPT keys per application.
1	Enabled	Financial keys are terminal based. For terminal based financial keys, SSA supports 64 Master/Session keys and 10 DUKPT keys per terminal.

Chapter 10

Secure Certificate

10.1 Overview

This chapter is extracted from the NAR Secure Certificate document, part 0190-00252-0103, revision 1.03.

The secure certificate file is a descriptor of all of the software components that are necessary to make up one or more applications that are going to be downloaded to the Secure PIN Entry Device, such as the i6500.

Terms used in this chapter are explained in *Terminal Architecture* on page 69.

10.2 Secure Certificate

If the secure Code MACing option is enabled, the downloaded application must provide what is called a “secure certificate file” (certific.txt). This file contains security information for every file and application to be downloaded. It can also indicate which application, code file, or data file needs to be deleted. This certificate is mandatory if Code MACing is enabled.

During the terminal download process, if the downloaded certificate file is valid and the download is successful, SSA will replace the previous copy, if it exists, with the new copy.

The secure certificate file will also be used each time the terminal starts up to authenticate the MAC of the user application’s CFS and DFS if the security option “Terminal Startup Verify MAC Option” is enabled.

The following section describes how the securing process uses the secure certificate and gives practical considerations for application developers.

10.3 Securing Process

The securing process can be used during the validation of the application code files and application data files.

The secure certificate will be downloaded into the data file system (DFS) first, along with code files and data files. The secure certificate contains all security-related information, and information about all of the code files and data files in the download package. The securing process is composed of the following steps:

1. The secure certificate is used to validate the complete download of all required download files. If Code MACing is enabled, downloading any file that is not listed in the secure certificate file causes the download to fail.

2. The maintenance application sends a request to SSA to validate the secure certificate file.

3. The secure certificate file is used to validate the signature of code files and data files as soon as they are installed. The secure certificate can also be accessed as needed throughout the download procedure.

4. If the download is successful, the secure certificate file will be erased from a temporary location and updated into SSA's memory.

10.4 Secure Certificate

The secure certificate is a text file that contains security information for a download package.

Once the text file is constructed, it must be passed through a securing utility which generates the MAC of the certificate. The utility will also generate MACs for all of the software components described in the certificate.

The secure certificate contains all the security information necessary for SSA to determine if the downloaded application is eligible to upgrade.

The secure certificate is also a descriptor of all the software components that are necessary to make up a download session. In effect, the secure certificate represents an application descriptor file that contains secured fingerprints for each of the software components representing the application.

The following is an example of a secure certificate text file.

```
MAC=12345678

[VisaPEDMode]
1

[Appl]
MAC=12345678 applname dstfilename.ext authmethod encrypt
srcfilename.ext

[SecFiles]
MAC=12345678 applname dstfilename.ext class authmethod encrypt
existence srcfilename.ext
MAC=12345678 applname dstfilename.ext class authmethod encrypt
existence srcfilename.ext

[NonSecFiles]
applname filename.ext class existence
applname filename.ext class existence

[DeleteAppl]
applname codefilename1
applname codefilename2

[DeleteFiles]
applname filename.ext class
applname filename.ext class

[DeleteWholeApp]
applname
```

Note: All lines within the secure certificate text file are terminated with a character sequence carriage return followed by line feed (e.g., <*cr*><*lf*>) ***except*** for the last line of the file.

The fields of the file are described more fully in the sections that follow.

10.5 Secure Certificate Descriptor Sections

The following descriptor sections make up a secure certificate:

- Secure certificate MAC descriptor section
- Visa PED mode descriptor section
- Application descriptor section
- Secure file descriptor section
- Non-secure file descriptor section
- Delete application code file descriptor section
- Delete data file descriptor section
- Delete the whole application descriptor section

10.5.1 Secure Certificate MAC Descriptor Section

This section, which is the MAC of the secure certificate file, must exist on the first line of the file. If it does not, validation fails. If it does, a MAC is calculated on the secure certificate, using SHA1 + MAC, starting from the first character of the second line of the file until the end of the file.

If the MAC detected on the first line of the file is not the same as the calculated MAC, validation fails.

The first line of the file must be in the following format:

```
MAC=12345678
```

The first field of the application descriptor is the MAC for the secure certificate file itself.

- *MAC*= is a text string indicating that the precalculated fingerprint follows
- *12345678* is the Hex ASCII representation of the most significant 4 bytes of the MAC value of the SHA1 result for the whole certificate file, precalculated and applied by the securing utility prior to download.

Note: The first line of the file must end with a carriage return and line feed. The second line is considered to begin at the first character immediately after the first carriage return and line feed characters of the file.

10.5.2 Visa PED Mode Descriptor Section

The Visa PED mode descriptor section allows you to set the terminal into a special mode that meets the Visa PIN encryption device (PED) requirements. Visa PED mode should be entered before downloading.

The section identifier *[VisaPedMode]*<*cr*><*lf*> marks the beginning of the Visa PED mode section within the file. The Visa PED Mode descriptor section is found after the secure certificate MAC section identifier and before the start of the next section identifier (i.e., encountered by <*cr*><*lf*>*[*).

The first line of the file must look like this:

```
mode
```

- *mode* represents the value of the Visa PED mode before the certificate file is updated and before the download starts.

Possible Values	Description
;	No security mode is set.
1 – 7 (00000B2B1 B0)	B0 – Visa PED mode B1 – Code MACing B2 – Prompt MACing
1 (000000001)	Visa PED mode. Visa PED mode will not be enabled if the secure text entry key and the clear text entry key are not injected, or if the download key is not injected.
2 (000000010)	Code MACing. Code MACing will not be enabled if the download key is not injected.
3 (000000011)	Visa PED mode and Code MACing. Visa PED mode and Code MACing will not be enabled if the secure text entry key and clear text entry key are not injected, or if the download key is not injected.
4 (000000100)	Prompt MACing. Prompt MACing will not be enabled if the secure text entry key and clear text entry key are not injected.
5 (000000101)	Visa PED Mode and Prompt MACing. This option will not be enabled if the secure text entry key and clear text entry key are not injected, or if the download key is not injected.
6 (000000110)	Prompt MACing and Code MACing. This option will not be enabled if the secure text entry key and clear text entry key are not injected, or if the download key is not injected.
7 (000000111)	Visa PED mode and Prompt MACing and Code MACing. This option will not be enabled if the secure text entry key and clear

	text entry key are not injected, or if download key is not injected.

The three security options (Visa PED Mode, Prompt MACing, and Code MACing) can only be turned off through the key injection module.

If the Visa PED mode section indicates to turn Visa PED mode on, but the platform code files (in the download package or terminal) cannot pass the authentication or cannot find MAC information in the certificate file, then Visa PED mode cannot turn on and the download fails.

If the Visa PED Mode section indicates to turn Code MACing on, but the platform and financial application code files (in the download package or terminal) cannot pass the authentication or cannot find MAC information in the certificate file, Code MACing cannot turn on and the download fails.

Note: The first line of the file must end with a carriage return and line feed.

The second line is considered to begin at the first character immediately after the first carriage return and line feed characters of the file.

10.5.3 Application Descriptor Section

The application descriptor section is an area of the secure certificate file that contains information pertaining to the application code files.

The section identifier *[Appl]<cr><lf>* marks the beginning of the application descriptor section within the file. The section ends before the start of the next section identifier (i.e., encountered by *<cr><lf>[*), or the end of the file.

There must be at least one application descriptor; otherwise, the secure validation process fails. Only the first application descriptor is accepted and parsed within the application section.

The application descriptor is in the format:

```
MAC=12345678 applname dstfilename.ext authmethod encrypt
srcfilename.ext
```

The first field of the application descriptor is the MAC for the application.

- *MAC*= is a text string identifying that the pre-calculated fingerprint follows
- *12345678* is the Hex ASCII representation of the most significant 4 bytes of the MAC applied by the securing utility prior to download.
- *applname* represents the application name of the application binary being loaded. For instance: CA2100_IBMEF
- *dstfilename.ext* represents the code file name of the application binary file residing in the terminal. For instance: WW002G011010
- *authmethod* represents the code file authentication method, i.e., the MAC calculation method that the code file used. Possible values:
    - SHA1+MAC

— CBC+MAC. Use Code Download MAC Key: CDMK XOR 0x0000 0000 0000 00FF for each half of the key to do MAC calculation/verification.

The MAC is calculated before the code file is encrypted. If the code file is specified to be encrypted, then the calculated data needs to be a multiple of 8 bytes. If it isn't, the generated encrypted code file will have zeros appended at the end of the file for MAC calculation.

- *encrypt* represents whether the code file is encrypted and needs to be decrypted. Possible values: Y, N. If the code file is encrypted, it should be encrypted under the variant of CDMK.

  The applied variant method is use CDMK XOR 0x0000 0000 0000 FF00 for each half of the key to do encryption/decryption.

  If the code file needs to be encrypted, the MAC value will be calculated and it will be added to the certificate file. Next, it will encrypt the code using the variant of CDMK starting from address 0x0200 (the code file header is not encrypted). If the code file is not a multiple of 8 bytes, the last data block will have zeros appended for encryption calculation. The number of zeros that are appended to the code file are also appended to the end of the output encrypt file (e.g., adds "4" to represent four zeros). An encrypted code file will be generated with extension '.enc'. The encrypted application code file thus consists of three portions:

  — The first 0x0200 bytes (i.e. 512 bytes) are the first 512 bytes of the original application code file in clear form.

  — The second portion is variable in length depending on the size of the original application code file. It consists of groups of encrypted data. Each group is of 8 bytes long. The last group is padded with 0's to make up 8 bytes, if necessary, before encryption.

  — The third portion is one byte long. Its value indicates the number of 0's padded to the last group of data. It is in clear form.

  — Note: Code file 0 won't be encrypted even if the encrypt field is specified to be "yes."

- *srcfilename.ext* represents the relative or full path of the code file residing in the computer. For instance: code\ WW002G011010. This field is not used by the secure process, but will be used by the securing utility.

10.5.4 Secure File Descriptor Section

The secure file descriptor section is an area of the secure certificate file that contains information pertaining to the files that require secure fingerprint validation.

By being able to define the files that require fingerprint validation, the developer can maintain some level of control over what and how much of the application needs to be validated.

Note: If an application has parameter files that could change dynamically from an external source, then these files can be defined in the non-secure section, thus escaping the rigors of fingerprint validation. The securing party has ultimate control over whether to

accept or reject such a configuration. This decision is made prior to MACing the secure certificate.

The secure file descriptor section is found after the identifier *[SecFiles]*<*cr*><*lf*> and before the next section identifier (i.e., encountered by <*cr*><*lf*>*[*), or end of the file. The secure file descriptor is in the format:

```
MAC=12345678 applname dstfilename.ext class authmethod encrypt
existence srcfilename.ext
```

The first field of the secure file descriptor is the MAC for the application data file.

- *MAC*= is a text string identifying that the pre-calculated fingerprint follows.
- *12345678* is the Hex ASCII representation of the most significant 4 bytes of the MAC applied by the securing utility prior to download.
- *applname* represents what application this data file belongs to.
- *dstfilename.ext* represents the relative path and file name where the data file will reside in the UNICAPT 32 file system. For instance: bitmaps/card.bmp
- *class* represents the particular categorization of the file within the terminal's file system. Possible values: 0=private, 1=public.
- *authmethod* represents the data file authentication method, i.e., the MAC calculation method that the data file used. Possible values:
  - SHA1+MAC
  - CBC+MAC. Use Code Download MAC Key: CDMK XOR 0x0000 0000 0000 00FF for each half of the key as the variant of CDMK to do MAC calculation/verification. The variant of CDMK that results from the XOR operation is used for both methods.

    The MAC is calculated before the data file is encrypted. If the data file is specified to be encrypted, then the calculated data needs to be a multiple of 8 bytes. If it isn't, the generated encrypted code file will have zeros appended at the end of the file for MAC calculation.
- *encrypt* represents whether the data file is encrypted and needs to be decrypted. Possible values: Y, N. If the data file is encrypted, it should be encrypted under the variant of CDMK.

  Use Code Download MAC Key: CDMK XOR 0x0000 0000 0000 00FF for each half of the key as the variant of CDMK to do encryption/decryption.

  If the data file is specified to be encrypted, the MAC value is calculated and then added to the certificate file. Next, it will encrypt the data using the variant of CDMK. If the data file is not a multiple of 8 bytes, the last data block will have zeros appended for encryption calculation. The number of zeros that are appended to the code file are also appended to the end of the output encrypt file (e.g., adds "4" to represent four zeros). An encrypted data file will be generated with extension '.enc'.

  The encrypted secure data file thus consists of two portions:

  - The first portion is variable in length, depending on the size of the

original application code file. It consists of groups of encrypted data. Each group is of 8 bytes long. If necessary, the last group is padded with zeros to make up 8 bytes before encryption.

— The second portion is one byte long. Its value indicates the number of zeros padded to the last group of data. It is in clear form.

- *existence* is an option to determine whether the file must exist in terminal memory in order for secure validation to succeed.
  - — "Y" indicates that the file must exist. If Y is selected and the file exists but does not validate, then the secure process fails.
  - — "N" indicates the file need not exist. If N is selected, then the file optionally may or may not exist for validation to succeed.
- *srcfilename.ext* represents the full or relative DOS path and file name that the data file binary resides in. This field is not used by the secure process, but may be used by the securing utility.

Note: When Visa PED Mode is on, the BIN configuration file has to be included in the Security File Section, and the applname should be SSA.

10.5.5 Non-Secure File Descriptor Section

The non-secure file descriptor section is an area of the secure certificate file that contains information pertaining to the files that do not require secure fingerprint validation.

All files of an application that have not been defined in the secure file section must be defined in the non-secure file section.

The non-secure file descriptor section begins with the descriptor *[NonSecFiles]<cr><lf>*. This section ends with the start of the next section header (i.e., encountered by *<cr><lf>[*), or end of the file. The non-secure file descriptor is in the format:

```
applname filename.ext class existence
```

- *applname* represents what application this data file belongs to.
- *filename.ext* represents the relative path and file name where the data file will reside in the UNICAPT 32 file system. For instance : bitmaps\card.bmp
- *class* represents the particular categorization of the file within the terminal's file system. Possible values: 0=private, 1=public.
- *existence* is an option to determine whether the file must exist in terminal memory in order for secure validation to succeed.
  - — "Y" indicates that the file must exist. If Y is selected and the file exists but does not validate, then the secure process fails.
  - — "N" indicates the file need not exist. If N is selected, then the file optionally may or may not exist for validation to succeed.

10.5.6 Delete Application Code File Descriptor Section

The delete application code file descriptor section is an area of the code to be deleted.

The delete application code file descriptor section begins with the descriptor *[DeleteAppl]<cr><lf>*. The section ends with the start of the next section header (i.e., encountered by "*<cr><lf>[*"), or end of the file. The delete code file descriptor is in the format:

```
applname codefilename
```

- *applname* represents the application that this code file belongs to.
- *codefilename* represents the code file that belongs to an application. For example, CA0003001000.

Note: The operating system, maintenance application, and System & Security Application cannot be deleted. Only the financial application can be deleted.

10.5.7 Delete Data File Descriptor Section

The delete data file descriptor section is an area of the data file that contains information pertaining to the files to be deleted.

The delete data file descriptor section begins with the descriptor *[DeleteFiles]<cr><lf>*. The section ends with the start of the next section header (i.e., encountered by *<cr><lf>[*), or end of the file. The delete file descriptor is in the format:

```
applname filename.ext class
```

- *applname* represents the application this data file belongs to.
- *filename.ext* represents the relative path and file name where the data file resides in the UNICAPT 32 file system. For instance: bitmaps\card.bmp
- *class* represents the particular categorization of the file within the terminal's file system. Possible values: 0=private, 1=public.

10.5.8 Delete Whole Application Descriptor Section

The delete whole application descriptor section is an area of application to be deleted.

The delete whole application descriptor section begins with the identifier *[DeleteWholeApp]<cr><lf>*. This section ends with the start of the next section header (i.e., encountered by *<cr><lf>[*), or end of the file. The delete whole application descriptor is in the format:

```
applname
```

- *applname* represents the application name that is going to be deleted. For example: US0901_UPOS.

Note: The operating system, maintenance application, and System & Security Application cannot be deleted. Only the financial application can be deleted.

Chapter 11

IBMEFT Download

11.1 Prerequisites

The prerequisites are:

- The ability to accept downloaded files and store on system.
- A download utility (IBMEFT or NCREFT - IBM EFT uses an IBM protocol for downloading, and NCR uses an NCR protocol for downloading).
- A POS system that supports IBMEFTDL, NCREFTDL, or equivalent functionality, as determined by your project manager.

  Note: IBMEFTDL is an Ingenico download utility that runs on the store controller or server. It downloads data through the ECR to the Ingenico 6500 using the IBMEFT protocol.

NCREFTDL is supported and managed directly by NCR for NCR customers.

11.2 Preparation

Ensure equipment is functional and in the right place:

- Ensure store network is operational
- Ensure each cash register is functional and connected to the network
- Ensure store controller has the ability to manage all download files and interface with each ECR
- Ensure that each Ingenico 6500 terminal is connected to an ECR
- Ensure that the application levels are the same in all Ingenico 6500 terminals

It is a good idea to download to a small number of terminals first.

11.3 Timing

To perform a download on an RS-232 Type A communication running at:

- 19200 bps, it takes approximately 25 minutes
- 9600 bps, it takes approximately 40 minutes

11.4 Outline of Download Process Steps

The download process is as follows:

1. Ensure that all Ingenico 6500 terminals operating in the store are running the same levels of software. If they are not, take note of the software levels (see section 4.2, *Finding Version* Numbers, on page 17), then check with your account manager before proceeding to see if additional testing is necessary.

2. Install all of the necessary Ingenico download utility and EFT files to the proper directory on the store controller or server.

3. From the store controller, initiate the download.

4. Sign onto each cash register that has an Ingenico 6500 terminal attached to it. The store controller will check for Ingenico 6500 EFT version levels. If the EFT version levels differ from the Ingenico 6500, the store controller will detect that and automatically update the software.

   Note: For stores that operate 24 hours, the process involves going to one unused register at a time, until every cash register and every Ingenico 6500 terminal is upgraded. Ask store management for cashier assistance to prevent interruption of store operations and facilitate awareness of progress.

   While the download is in process at a terminal, it cannot be used to process transactions.

11.4.1 Feedback

Depending on your cash register configuration, the i6500 terminal may not be used if PROGxxxx/PARMxxxx is displayed during download. If no message is displayed in the cashier display, debit and credit transactions cannot be processed.

It is critical to execute a systematic incremental procedure in order to ensure consistency of download on all units in store. For assistance in the preparation to implement a multiple-unit simultaneous download procedure, please contact your Ingenico Project Manager.

If a power outage or glitch occurs during the download, or if you disconnect the Ingenico 6500 terminal during the download, the terminal will cease to function. If the disruption occurred during the upgrade of the System & Security Application, the terminal will need to be sent to an authorized repair facility for recovery (contact your project manager).

Monitor both the store controller and Ingenico 6500 terminal during the download process.

If the download fails, it will assist troubleshooting efforts to know at what point the download failed and to record what error code displays on either the store controller or on the 6500 terminal display.

To run your batch file:

1. Ensure the Ingenico 6500 terminals are in the ready state.

2. Load files into the store controller's PIN pad program directory.

3. Initiate a download from the controller.

   The cashier display details activity and status updates, such as "Downloading, PROG xxxx" or "Downloading PARM xxxx."

   The Ingenico 6500 terminal indicates a summary of its activity, "IBM EFT prog Dowld.blk ##." When complete, the cashier display reads "Closed" or "Enter Item." The Ingenico 6500 terminal goes into the online or offline state.

4. Ensure that all Ingenico 6500 terminals that have attempted an IBMEFTDL or parameter level upgrade are running the proper levels of software (see section 4.2, Finding Version Numbers, on page 17). Record discrepancies if any are found to have failed acceptance of the download and note the location of the device. If a download fails, always conduct a second download attempt and report second failures to your Ingenico Project Manager.

5. Check the properties of the communications port to make sure that the interrupt request and input/output range has not been changed.

Chapter 12

Download Errors

12.1 Error Opening Port

This error message displays on the computer or cash register. The following sections list possible causes and corresponding solutions.

12.1.1 The communications port that IBMEFTDL is using is already being used by another application

Close the other application and run the download file again.

12.1.2 The communications port is not working

- Try another computer.
- Ask your Ingenico representative to change the batch file to work with the new communications port. Change to the new communications port, then run the new batch file.

12.1.3 The hardware settings in the Ingenico 6500 have been changed

1. Check the properties of the communications port to make sure that the interrupt request and input/output range has not been changed. In Windows 98 or 2000:

   a. Right-click **My Computer**, then select **Properties**.

   b. Click the **Device Manager** tab.

   c. From the list, double-click **Ports**, double-click **Communications Ports**, and then go to the **Resources** tab.

2. Ensure the settings for COM1 are the default, as follows:

   - **Interrupt Request** is **04**
   - **Input/Output Range** is **03F8**

3. Ensure the settings for COM2 are the default, as follows:

   - **Interrupt Request** is **03**
   - **Input/Output Range** is **02F8**

12.2 Received 3 NAKs or Timeout in sendVISAPacket()

This error message displays on the computer or cash register. The following sections list possible causes and corresponding solutions.

12.2.1 There may be a loose connection between the host and the Ingenico 6500

Ensure the cables are securely connected.

12.2.2 The communications port settings and EFT/NCR protocol setting in the Ingenico 6500 may be wrong

The following procedure explains how to compare the configuration that you have in your IBMEFTDL file to make sure that it is the same as the default setup configuration in your Ingenico 6500 terminal (for details, see 12.3 *Default Setup Configuration* on page 98).

1. To find the communication port settings in your IBMEFTDL file, open the download batch file, search for the keyword "ibmeftdl", and find the following parameters:

    - /b: the number following this parameter is the required RS232 baud rate.
    - /d: the number following this parameter is the required RS232 data bits.
    - /t: the character following this parameter is the required RS232 parity setting. An "n" means none parity, "e" means even, "o" means odd parity.

2. Write these parameters down.

3. Next, go the Ingenico 6500 terminal to read the current settings to see if they are the same. Restart the terminal by pressing [1] + [OK] + [CAN]; while it is restarting, access the Extended Menu by pressing [1] and [3] simultaneously.

4. Select **System Info**, and then select **View Parameter**. The screen displays the current download configuration for the port the terminal has configured to do the download, the baud rate, data bits, stop bits, and parity of that port.

5. Compare these settings to the IBMEFTDL parameters that you wrote down in step 2; they should be the same. If not, change them using the following steps.

6. From the Communications menu, press [Can] twice to return to the **Supervisor Menu**. Enter the password, select **System Parameters,** and then select **Download Method**. Select IBMEFT or NCREFT.

7. Press [Can] to return to the **System Parameters** menu**,** and then select **Download Port**. Select the correct download port and correct communication type.

8. Press [Can] to return to the **System Parameters** menu**,** and then select **Setup Port**. Select the port to setup, and select the correct baud rate, data bits, stop bits, and parity.

9. After all the settings are updated, the terminal will update the system parameter setting, when you exit the extended menu, the terminal will reset.

12.3 Default Setup Configuration

Configuration	Default Value
IBMEFT/NCR protocol selection	IBMEFT
Download Port Number	Com1
Download Port Type	RS232
RS232 baud rate	19200
RS232 data bits	8
RS232 parity	No parity
RS232 stop bits	1

12.4 Error: Bad Prog.

The flash memory in the terminal may not match the flash memory requirement of EFTL file. Contact your account manager to arrange to have the terminal sent in for repair.

12.5 Device already loaded with program x and parameter y

This error message displays on the computer or cash register if the Ingenico 6500 has already been upgraded.

12.6 CRC Error

The CRC Error message, followed by multiple characters in a string, displays on the Ingenico 6500 to indicate that the Security Module has been compromised. Notate error to report with issue. Notify your Ingenico Project Manager immediately and request RMA number authorization to return unit to an authorized repair facility for recovery.

12.7 Not Enough DFS Space

This error occurs during a download if the Ingenico 6500 terminal's data file system does not have enough space to receive any additional download components. To resolve the error, clean up the DFS to make room for downloads. There are two ways to do this:

- Use MLDT or Wingload 32 to get the DFS information from the terminal and manually delete any redundant files.
- Go to the Core Menu (or Production Menu) by restarting the terminal and pressing the top left corner of the screen while the terminal is starting up. Select **AdvancedOptions**, enter the password, and then select **FormatDFS**. ***This method will reformat the data file system and delete all existing data files.***

12.8 Comm Receive Error

This error occurs when the terminal doesn't receive a message from the host within the timeout period. To resolve the error, extend the Response TMO setting in the terminal or host.

Chapter 13

IBM EFT Troubleshooting

This section describes how to resolve error messages that may appear on your Ingenico 6500 device display if using IBMEFTDL.

13.1 Card Read Error1

If the Card Read Error message displays on the device after swiping a card through the MSR:

- Try swiping the card a few more times, varying the speed at which the card is physically drawn through the reader.
- Try swiping the card in the reverse direction (i.e., if swiping the card from top to bottom, try swiping the card from bottom to top, front to back: back to front).
- Make sure that you are swiping the card in a straight line (i.e., make sure the MSR card is always touching the bottom of the MSR track).
- If none of these actions work, then the MSR card is worn and cannot be read electronically. Enter the card number manually.
- If the register is reloaded immediately after powering up, the Ingenico 6500 may not come up in the correct state. Signing in at the register and seeing if the Ingenico 6500 display reads “Please Slide Card” can determine this. If it does not (i.e., display continues to read, “Closed”), then perform the same steps as for the next error message, EFT Device Not Available.

13.2 EFT Device Not Available

If the EFT Device Not Available message displays on the register, perform the following steps:

1. Check to make sure the Ingenico 6500 is on and is displaying the first prompt screen of your application software.
2. On the register, press the **Clear** key and select the transaction type again. If the problem persists, continue to step 3.
3. To restart the Ingenico 6500 device, press **Cancel + 0 + Enter** simultaneously.

   The Ingenico 6500 restarts and the first prompt screen of the application software displays.
4. On the register, press the **Clear** key and select either the CREDIT or DEBIT transaction type again.

The Ingenico 6500 should now be at the first prompt screen of your application software (i.e., it now reads “Please Slide Card”). If not, sign off the register and then sign on again.

13.3 EFT Device Not Available – During Check Authorization

If the EFT Device Not Available message displays on the register during check authorization:

1. Check to make sure the Ingenico 6500 is on and is displaying the first prompt screen of your application software.
2. On the register, press the **Clear** key and select the transaction type again. If the problem persists, continue to step 3.
3. To restart the Ingenico 6500 device, press **Cancel + 0 + Enter** simultaneously.

   The Ingenico 6500 restarts and the first prompt screen of the application software displays.
4. On the register, press the **Clear** key and select the CHECK transaction type.

The Ingenico 6500 should now be at the first prompt screen of your application software (i.e., it now reads “Please Slide Card”). If not, sign off the register and then sign on again.